Efficient IBE with Tight Reduction to Standard Assumption in the Multi-challenge Setting

Junqing Gong[1], Xiaolei Dong[2](✉), Jie Chen[3,4,5](✉), and Zhenfu Cao[2](✉)

[1] Department of Computer Science and Engineering,
Shanghai Jiao Tong University, Shanghai, China
gongjunqing@126.com

[2] Shanghai Key Lab for Trustworthy Computing,
East China Normal University, Shanghai, China
{dongxiaolei, zfcao}@sei.ecnu.edu.cn

[3] School of Computer Science and Software Engineering,
East China Normal University, Shanghai, China
S080001@e.ntu.edu.sg, http://www.jchen.top

[4] École Normale Supérieure de Lyon, Laboratoire LIP, France

[5] College of Information Science and Technology, Jinan University, China

Abstract. In 2015, Hofheinz *et al.* [PKC, 2015] extended Chen and Wee's almost-tight reduction technique for identity based encryptions (IBE) [CRYPTO, 2013] to the multi-instance, multi-ciphertext (MIMC, or multi-challenge) setting, where the adversary is allowed to obtain multiple challenge ciphertexts from multiple IBE instances, and gave the first almost-tightly secure IBE in this setting using composite-order bilinear groups. Several prime-order realizations were proposed lately. However there seems to be a dilemma of high system performance (involving ciphertext/key size and encryption/decryption cost) or weak/standard security assumptions. A natural question is: can we achieve high performance without relying on stronger/non-standard assumptions?

In this paper, we answer the question in the affirmative by describing a prime-order IBE scheme with the same performance as the most efficient solutions so far but whose security still relies on the *standard* k-linear (k-Lin) assumption. Our technical start point is Blazy *et al.*'s almost-tightly secure IBE [CRYPTO, 2014]. We revisit their concrete IBE scheme and associate it with the framework of nested dual system group. This allows us to extend Blazy *et al.*'s almost-tightly secure IBE to the MIMC setting using Gong *et al.*'s method [PKC, 2016]. We emphasize that, when instantiating our construction by the Symmetric eXternal Diffie-Hellman assumption (SXDH = 1-Lin), we obtain the most efficient concrete IBE scheme with almost-tight reduction in the MIMC setting, whose performance is even comparable to the most efficient IBE in the classical model (i.e., the single-instance, single-ciphertext setting). Besides pursuing high performance, our IBE scheme also achieves a weaker form of anonymity pointed out by Attrapadung *et al.* [AsiaCrypt, 2015].

Keywords: Identity based encryption, Tight security, Multi-challenge setting, Nested dual system group, Prime-order bilinear group, Groth-Sahai proof system, (Weak) Anonymity

1 Introduction

1.1 Background and Motivation

The notion of identity based encryption (IBE) was proposed by Shamir [32] in 1984 and realized by Boneh and Franklin [7] in 2001 using bilinear groups. In an IBE system, an authority publishes a set of public parameters and issues secret keys for users according to their identities, the encryption requires the public parameters and receiver's identity (for example, his/her e-mail address). As an advantage over traditional PKI-based cryptosystems, users in an IBE system only need to authenticate and store the system-level public parameter once and for all, while users' identities are always self-explained and thus easy to validate.

Since Boneh and Franklin's work [7], a series of constructions [6, 5, 33, 13] appeared making trade-off between several features such as security model, strength of complexity assumption, and public key size. In 2009, Waters [34] proposed a novel proof technique, called *dual system encryption*, and showed the first adaptively secure IBE scheme with constant-size public key and polynomially related to the k-linear (k-Lin) assumption, a standard assumption, in the standard model. Nowadays the dual system technique has become a regular and powerful tool for achieving adaptive security of attribute based encryptions (ABE) and inner-product encryption (IPE) (and more general primitives) in the standard model [21, 26, 22, 28, 27]. More importantly, under the framework of dual system encryption, we have obtained a clean, deep, and uniform understanding on the construction of a branch of encryption systems, including IBE, ABE, IPE and so on [1, 35, 2, 8].

The classical adaptive security model for IBE [7] requires that the challenge ciphertext for the challenge identity reveals nothing even when the adversary has held secret keys for other identities. The dual system technique [34] generally works as follows. There are two forms of secret keys and ciphertexts, *normal* and *semi-functional* form. The normal ciphertexts/keys are used in the real system, while the semi-functional ciphertexts/keys are often constructed by introducing extra entropy into normal ones and will only be used for the security proof. We say normal object is in the normal space and the extra entropy is in the semi-functional space and require that they are independent in some sense. The proof follows the hybrid argument method. One first transforms the challenge ciphertext from normal to its semi-functional form. Next, one converts secret keys from normal to semi-functional form in an one-by-one fashion. Finally, one can immediately prove the security utilizing the extra entropy we have introduced in the semi-functional space.

Tight Security. Clearly, the reduction described above suffers from a security loss proportional to the number of secret keys the adversary held. Due to the generality of such a loss, a natural question is whether such a security loss is inherent for IBE in the standard model under standard assumptions? In practical point of view, a tightly secure IBE allows practitioners to implement this system in a smaller group, which always leads to shorter ciphertexts/keys and faster encryption/decryption operations in the real world.

Fortunately, Chen and Wee [9] answered the question in the negative. They proposed the first almost-tightly secure IBE in the standard model based on the k-Lin assumption. Here the so-called *almost-tight* means the security loss is proportional to the security parameter instead of the amount of secret keys revealed to the adversary. Technically, they combined the high-level idea of dual system encryption with the proof technique of Naor and Reingold [25]. In the next year, Blazy *et al.* showed an almost-tightly secure IBE with higher space and time efficiency. In fact, they proved that an adaptively secure IBE can be generically constructed from affine message authentication code (MAC) and Groth-Sahai non-interactive zero-knowledge (NIZK) proof [15], and offered us a realization of affine MAC based on Naor and Reingold's proof technique [25]. Roughly speaking, their high-level strategy is still identical to Chen and Wee's [9].

Let us take a look at Chen and Wee's idea [9]. Essentially, they borrowed the proof strategy from Naor and Reingold [25] in order to introduce entropy into semi-functional space more quickly. After converting normal ciphertext to semi-functional form, one may conceptually introduce a truly random function RF to all secret keys and challenge ciphertext whose domain is just $\{\epsilon\}$, i.e., unrelated to the identity. Relying on the binary encoding of the identities in secret keys, one can increase the dependency of RF on the identity, from 0-bit prefix to 1-bit prefix, 2-bit prefix, ..., and finally the entire identity. They called such a property *nested hiding*. At this moment, $\mathsf{RF}(\textsc{id})$ is revealed to adversary through secret key for $\textsc{id}$ while $\mathsf{RF}(\textsc{id}^*)$ for the challenge identity $\textsc{id}^*$ is still unpredictable since adversary is not allowed to hold its secret key. This feature is sufficient for proving the security. It is worth noting that for an identity space $\{0,1\}^n$, we just need n steps to construct such a random function RF and just arise $\mathcal{O}(n)$ security loss.

Multi-instance, Multi-ciphertext Setting. The classical security model for IBE [7] requires that the *single* challenge ciphertext from the *single* challenge identity should leak nothing about the corresponding message even with secret keys for adversarially-chosen identities. In 2015, Hofheinz *et al.* [18] considered a more realistic security model, called adaptive security in the *multi-instance, multi-ciphertext setting* (MIMC, or multi-challenge setting), which ensures the security of *multiple* challenge ciphertexts for *multiple* challenge identities in *multiple* IBE instances. In general, an IBE scheme secure in the classical single-instance, single-ciphertext (SISC) model must be secure in the MIMC setting. However the implication is *not* tightness-preserving. Assuming the number of IBE instances and challenge ciphertexts per instance are μ and Q, the general reduction from MIMC to SISC will arise a multiplicative security loss $\mathcal{O}(Q\mu)$.

Hofheniz *et al.* [18] extended Chen and Wee's tight reduction technique [9] and gave the first almost-tight secure IBE in the MIMC setting. Technically, the ηth *nested hiding* step in Chen and Wee's proof procedure requires that the ηth bit of all challenge identities should be identical. It is the case in the SISC setting but is not necessarily hold in the MIMC setting. To overcome this difficulty, they introduced another semi-functional space. Now the original semi-functional space may be called $\wedge$-semi-functional space and the new-comer may be named $\sim$-semi-functional space. They also employed two independent random functions $\widehat{\mathsf{RF}}$ and $\widetilde{\mathsf{RF}}$ for them, respectively, acting the same role of RF in Chen and Wee's proof. As the preparation for the ηth nested hiding, they transfer the entropy in $\wedge$-semi-functional space to $\sim$-semi-functional space for all challenge ciphertexts whose identity has 1 on its ηth bit. At this moment, we reach the configuration that, in every semi-functional spaces, the challenge identities indeed share the same ηth bit, and nested hiding can be done as Chen and Wee did but in each of two semi-functional spaces *independently.*

However their construction was built in composite-order bilinear groups. Attrapadung *et al.* [3] and Gong *et al.* [14] gave prime-order solutions independently. Attrapadung *et al.* [3] provided a generic framework building almost-tight secure IBE from *broadcast encoding* which is compatible with both composite-order and prime-order bilinear groups. Utilizing the power of broadcast encoding, they proposed not only ordinary IBE scheme but also IBE with other features such as sublinear-size master public key. Gong *et al.* [14] followed the line of extended nested dual system groups (ENDSG) [18] and proposed two constructions from more general assumptions, the second of which is an improved version based on the first one. In this paper, we do not consider additional feature and name Attrapadung *et al.*'s basic IBE in the prime-order group (i.e., $\mathit{\Phi}^{\mathsf{prime}}_{\mathsf{cc}}$) [3] as AHY, while name Gong *et al.*'s two constructions [14] as GCDCT and $\mathsf{GCDCT}+$.

Motivation. Among existing prime-order IBE constructions with almost-tight reduction in the MIMC model, there is a trade-off between the efficiency and strength of complexity assumption. On one hand, GCDCT was proven secure based on the k-Lin assumption but less efficient in terms of both ciphertext/key size and encryption/decryption cost. On the other hand, $\mathsf{GCDCT}+$ and AHY were more efficient but relied on the k-linear assumption with auxiliary input (k-LinAI) in asymmetric bilinear groups and the decisional linear assumption (sDLIN) in symmetric bilinear groups, respectively, which are stronger and less general than the k-Lin assumption. Therefore it is still an interesting and nontrivial problem to find a solution with some real improvements instead of just a trade-off. More concretely, we ask the following question:

Question: Can we find a tightly secure IBE scheme in the MIMC setting, which is (at least) as efficient as $\mathsf{GCDCT}+$ and AHY but still proven secure under the standard k-Lin assumption as GCDCT?

1.2 Our Main Result

In this paper, we answer the question in the affirmative by proposing an IBE scheme using prime-order bilinear groups in the MIMC setting. The adaptive security of the construction is almost-tightly based on the k-Lin assumption as GCDCT. At the same time, its performance is better than GCDCT and is identical to $\mathsf{GCDCT}+$ and AHY for corresponding parameter.

We compare existing almost-tightly secure IBE in prime-order groups with ours in detail in Table 1. The comparison involves the complexity assumption, the sizes of master public key, secret keys and ciphertexts, and encryption/decryption cost. As a base line, we also investigate almost-tightly secure prime-order IBE by Chen and Wee [9], denoted by CW, and Blazy *et al.* [4], denoted by BKP, both of which are adaptively secure in the SISC setting.

Table 1. Comparison among almost-tight IBE schemes in the prime-order group.

Scheme	**Sec.**	$\lvert\textsc{mpk}\rvert$		$\lvert\textsc{sk}\rvert$	$\lvert\textsc{ct}\rvert$		T_{Enc}		T_{Dec}	**MIMC**
		G_1/G	G_T	G_2/G	G_1/G	G_T	E_1/E	E_T	P	
CW	k-Lin	$2k^2(2n+1)$	k	$4k$	$4k$	1	$4k^2$	k	$4k$	✗
	DLIN	$16n+8$	2	8	8	1	16	2	8	
	SXDH	$4n+2$	1	4	4	1	4	1	4	
BKP	k-Lin	$k^2(2n+1)+k$	k	$2k+1$	$2k+1$	1	$2k^2+1$	k	$2k+1$	✗
	DLIN	$8n+6$	2	5	5	1	9	2	5	
	SXDH	$2n+2$	1	3	3	1	3	1	3	
GCDCT	k-Lin	$3k^2(2n+1)$	k	$6k$	$6k$	1	$6k^2$	k	$6k$	✔
	DLIN	$24n+12$	2	12	12	1	24	2	12	
	SXDH	$6n+3$	1	6	6	1	6	1	6	
GCDCT+	k-LinAI	$2k^2(2n+1)$	k	$4k$	$4k$	1	$4k^2$	k	$4k$	✔
	XDLIN	$16n+8$	2	8	8	1	16	2	8	
AHY	sDLIN	$16n+8$	2	8	8	1	16	2	8	✔
Ours	k-Lin	$k^2(2n+3)$	k	$4k$	$4k$	1	$4k^2$	k	$4k$	✔
	DLIN	$8n+12$	2	8	8	1	16	2	8	
	SXDH	$2n+3$	1	4	4	1	4	1	4	

- All schemes take $\{0,1\}^n$ as identity space.
- "DLIN" and "sDLIN" in Column "Sec." stand for decisional linear assumption in asymmetric and symmetric bilinear groups, respectively.
- Column $\lvert\textsc{mpk}\rvert$, $\lvert\textsc{sk}\rvert$, and $\lvert\textsc{ct}\rvert$ present numbers of group elements in master public keys, secret keys and ciphertexts, respectively. Here G refers to the source group of symmetric bilinear groups; G_1, G_2 are those of asymmetric bilinear groups; G_T stands for the target group for both cases.
- Column T_{Enc} and T_{Dec} give numbers of costly operations required during encryption and decryption procedures. E_1, E and E_T refer to exponentiation on the first source group of asymmetric bilinear groups, the only source group of symmetric bilinear groups, and target group in both cases, respectively. P is for pairing operation for both cases.

Benefit of Standard k-Lin. Compared with k-Lin, the k-LinAI assumption (used by GCDCT+) is not well-understood[6] and the sDLIN assumption (used by AHY) is stronger especially in the case of AHY[7]. Without doubt k-Lin is the

[6] The k-LinAI assumption is an extended (and stronger) version of k-Lin. However only its generic security has been investigated in [14].

[7] One may convert AHY into an asymmetric bilinear group and the security now relies on the XDLIN assumption, which is stronger than 2-Lin. Furthermore it's of course stronger than k-Lin for $k > 2$.

best choice. However we want to emphasize that achieving the same performance (as GCDCT+ and AHY) under the k-Lin assumption is not just advantageous to theorist, since we can indeed derive a strictly more efficient instantiation than all previous solutions. We note that, AHY is based on the sDLIN assumption and no related generalization was given, while the k-LinAI assumption, on which GCDCT+ is built, is not well-defined[8] for $k = 1$. In contrast, our construction can be naturally instantiated by $k = 1$ and yield an IBE scheme based on SXDH (see Section 6), whose performance is shown in the last row (in gray) of the table. Clearly, it has the shortest secret key/ciphertext and the most efficient encryption/decryption algorithm. Compared with BKP under the SXDH assumption, the cost we pay for stronger and more practical MIMC security is quite small: just one more group element is added to secret keys and ciphertexts, and just one more exponentiation and pairing operation are added to encryption and decryption procedure, respectively.

(Weak) Anonymity. Apart from the concern on performance, our main construction achieves anonymity as BKP and AHY. However the notion here is weaker than the standard anonymity, which was first pointed out by Attrapadung *et al.* [3]. All of them are proven to be anonymous under the restriction that all secret keys for the same identity must be created using the same random coin. It's reported in [3] that this can be fulfilled by generating the random coin using a PRF from each identity. A subtlety here is the newly introduced PRF itself should be tightly secure otherwise our effort pursuing tight security will finally come to nothing. In the paper we continue working in this restricted model and neglect this subtlety to keep a clean exposition.

1.3 Our Method

All of AHY, GCDCT, and GCDCT+ are extended from Chen and Wee's construction [9] or its recent development by Chen *et al.* [8]. However, from Figure 1, we can see that BKP, Blazy *et al.*'s almost-tightly secure IBE in the SISC model [4], is more efficient in terms of both space and time efficiency. Therefore our idea is to extend BKP to the MIMC setting and we hope that the resulting construction inherits its high performance and could become a solution to the problem we posed in Section 1.1.

Although Blazy *et al.* essentially followed the dual system technique, their concrete realization relied on the Groth-Sahai NIZK proof system [15], which is very different from constructions in [8, 9], the common bases of AHY, GCDCT, and GCDCT+. The existing extension strategy seemingly can not be directly applied to updating BKP to the MIMC setting.

To circumvent the difficulty, we reconsider BKP and observe a surprising connection between BKP and Chen *et al.*'s (non-tight) IBE [8]. This allows us to study and manipulate BKP in the framework of nested dual system groups

[8] The improvement technique behind GCDCT+ does not work for the special case $k = 1$ since two semi-functional spaces are 1-dimension and too small to compress.

(NDSG) [9] which is much easier to understand and also more feasible to extend towards the MIMC setting [18, 14] with existing techniques. We provide the reader with a technical overview in Section 3 covering our basic observation and sketching our two technical results which formally treat the observation.

1.4 Related Work

In 2013, Jutla and Roy [19] investigated the notion of quasi-adpative NIZK (QANIZK) and developed an IBE scheme from their SXDH based QANIZK. Both this work and Blazy *et al.*'s work [4] realized the dual system technique using NIZK proof and the idea is actually quite similar. Blazy *et al.* focused on generic frameworks from affine MAC to IBE, while Jutla and Roy considered many other applications of newly proposed QANIZK. A series of work [30, 31, 29] extended Jutla and Roy's IBE constructions to more complex functionality.

Since being introduced in 2013, Chen and Wee's technique of almost-tight reduction [9] has been applied to other primitives such as public key encryption against chosen-ciphertext attack and a signature [23] and QANIZK with unbounded simulation soundness [24]. Recently, Hofheinz [17, 16] proposed a series of novel techniques based on Chen and Wee's [9] and achieved constant-size parameters and better efficiency for public key encryptions with chosen-ciphertext security and signatures. In the pairing-free setting, Gay *et al.* [12] provided more efficient CCA secure PKE with tight reduction and applied their basic idea to NIZK proof system.

Roadmap. We review necessary preliminary background in Section 2. Section 3 is an overview with more technical detail. Section 4 and Section 5 present our two technical results. We show our main result (from k-Lin assumption) and its concrete instantiation under SXDH assumption in Section 6.

2 Preliminaries

Notation. We use $a \leftarrow A$ to denote the process of uniformly sampling an element from set A and assigning it to variable a. We employ $\{x_i\}_{i \in I}$ to denote a family (or list) of objects with index set I. The abbreviation $\{x_i\}$ will be used when index set is clear in the context. Let G be a group of order p. Given two vectors $\mathbf{a} = (a_1, \ldots, b_n) \in G^n$ and $\mathbf{b} = (b_1, \ldots, b_n) \in G^n$, we let $\mathbf{a} \cdot \mathbf{b} = (a_1 b_1, \ldots, a_n b_n) \in G^n$. For $\mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{Z}_p$ and $g \in G$, we define $g^{\mathbf{c}} = (g^{c_1}, \ldots, g^{c_n}) \in G^n$. For any matrix $\mathbf{A} \in \mathbb{Z}_p^{m \times n}$ with $m > n$, we use $\overline{\mathbf{A}}$ to refer to the square matrix consisting of the first n rows of $\mathbf{A}$ and let $\underline{\mathbf{A}}$ be the sub-matrix consisting of the remaining $m - n$ rows. For any square matrix $\mathbf{A} \in \mathbb{Z}_p^{m \times m}$, we define $\mathbf{A}^* = (\mathbf{A}^\top)^{-1}$. We use $(\mathbf{A}|\mathbf{B})$ to denote the matrix formed by concatenating columns of matrix $\mathbf{A}$ and $\mathbf{B}$ in order.

2.1 Prime-order Bilinear Group

Let GrpGen be a prime-order bilinear group generator which takes as input security parameter 1^λ and outputs group description $\mathcal{G} = (G_1, G_2, G_T, p, e, g_1, g_2)$.

Here G_1, G_2 and G_T are finite cyclic groups of prime order p and $|p| = \Theta(\lambda)$. $e : G_1 \times G_2 \to G_T$ is an admissible (non-degenerated and efficiently computable) bilinear map. g_1, g_2 and $g_T = e(g_1, g_2)$ are respective generators of G_1, G_2, G_T. We employ the *implicit representation* of group elements [11]. For any $a \in \mathbb{Z}_p$ and any $s \in \{1, 2, T\}$, we define $[a]_s = g_s^a \in G_s$. For any matrix $\mathbf{A} = (a_{i,j}) \in \mathbb{Z}_p^{m \times n}$, we define $[\mathbf{A}]_s = ([a_{i,j}]_s) \in G_s^{m \times n}$ and let $e([\mathbf{A}]_1, [\mathbf{B}]_2) = [\mathbf{A}^\top \mathbf{B}]_T$ when $\mathbf{A}^\top \mathbf{B}$ is well-defined.

The security of our construction relies on the *Matrix Decisional Diffie-Hellman* (MDDH) Assumption introduced in [11].

Definition 1 (Matrix Distribution [11]). *For any $\ell, k \in \mathbb{N}$ with $\ell > k$, we let $\mathcal{D}_{\ell,k}$ be a matrix distribution over all full-rank matrices in $\mathbb{Z}_p^{\ell \times k}$. Furthermore, we assume the first k rows of the output matrix form an invertible matrix.*

Assumption 1 ($\mathcal{D}_{\ell,k}$-Matrix Diffie-Hellman Assumption [11]) *Let $\mathcal{D}_{\ell,k}$ be a matrix distribution and $s \in \{1, 2, T\}$. For any p.p.t. adversary $\mathcal{A}$ against GrpGen, the following advantage function is negligible in λ.*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathcal{D}_{\ell,k}}(\lambda) = |\Pr[\mathcal{A}(\mathcal{G}, [\mathbf{A}]_s, [\mathbf{Au}]_s) = 1] - \Pr[\mathcal{A}(\mathcal{G}, [\mathbf{A}]_s, [\mathbf{v}]_s) = 1]|$$

where $\mathcal{G} \leftarrow \mathsf{GrpGen}(1^\lambda)$, $\mathbf{A} \leftarrow \mathcal{D}_{\ell,k}$, $\mathbf{u} \leftarrow \mathbb{Z}_p^k$, $\mathbf{v} \leftarrow \mathbb{Z}_p^\ell$.

The matrix distribution $\mathcal{D}_{k+1,k}$ will extensively appear in the paper. For simplicity, we take $\mathcal{D}_k$ as its abbreviation. As in [8], we let $\mathcal{D}_k$ output an additional vector $\mathbf{a}^\perp \in \mathbb{Z}_p^{k+1}$ satisfying $\mathbf{A}^\top \mathbf{a}^\perp = \mathbf{0}$ and $\mathbf{a}^\perp \neq \mathbf{0}$. The notable *$k$-Linear* ($k$-Lin) Assumption is a special case of the $\mathcal{D}_k$-MDDH assumption with

$$\mathbf{A} = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_k \\ 1 & \cdots & 1 \end{pmatrix} \in \mathbb{Z}_p^{(k+1)\times k} \quad \text{and} \quad \mathbf{a}^\perp = \begin{pmatrix} a_1^{-1} \\ \vdots \\ a_k^{-1} \\ -1 \end{pmatrix} \in \mathbb{Z}_p^{k+1}$$

where $a_1, \ldots, a_k \leftarrow \mathbb{Z}_p$. We describe a lemma similar to that shown in [8].

Lemma 1. *With probability $1 - 1/p$ over $(\mathbf{A}, \mathbf{a}^\perp) \leftarrow \mathcal{D}_k$ and $\mathbf{b} \leftarrow \mathbb{Z}_p^{k+1}$, we have*

$$\mathbf{b} \notin \mathsf{Span}(\mathbf{A}) \quad \textit{and} \quad \mathbf{b}^\top \mathbf{a}^\perp \neq 0.$$

We will heavily use the uniform matrix distribution $\mathcal{U}_{\ell,k}$, which uniformly samples a matrix over $\mathbb{Z}_p^{\ell \times k}$. Similarly, we let $\mathcal{U}_k$ be the short form of $\mathcal{U}_{k+1,k}$. A direct observation is "$\mathcal{D}_k$-MDDH $\Rightarrow$ $\mathcal{U}_k$-MDDH" with constant security loss, since any $\mathcal{D}_k$-MDDH instance can be disguised as a $\mathcal{U}_k$-MDDH instance using a random square matrix (c.f. [11, 12]). Besides, we have the following lemma.

Lemma 2 ($\mathcal{U}_k \Rightarrow \mathcal{U}_{\ell,k}$, $\ell > k$ [12]). *For any p.p.t. adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$ with $\mathsf{T}(\mathcal{B}) \approx \mathsf{T}(\mathcal{A}) + k^2\ell \cdot \mathsf{poly}(\lambda)$ and*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathcal{U}_{\ell,k}\text{-MDDH}}(\lambda) \leq \mathsf{Adv}_{\mathcal{B}}^{\mathcal{U}_k\text{-MDDH}}(\lambda).$$

The observation and the lemma lead to the fact that $\mathcal{U}_{\ell,k}$-MDDH with $\ell > k$ is *constantly* implied by the well-known k-Lin assumption. In the paper, we utilize the following structural lemma [12].

Lemma 3. *For a fixed full-rank* $\mathbf{A} \in \mathbb{Z}_p^{3k\times k}$*, with probability at least* $1 - 2k/p$ *over* $\widehat{\mathbf{A}}, \widetilde{\mathbf{A}} \leftarrow \mathcal{U}_{3k,k}$*, we have* $\mathsf{Span}\big((\mathbf{A}|\widehat{\mathbf{A}}|\widetilde{\mathbf{A}})\big) = \mathbb{Z}_p^{3k}$*, in which case it holds that*

$$\mathsf{Span}(\mathbf{A}^{\perp}) = \mathsf{Ker}\big((\mathbf{A}|\widehat{\mathbf{A}})^{\top}\big) \oplus \mathsf{Ker}\big((\mathbf{A}|\widetilde{\mathbf{A}})^{\top}\big).$$

and $\widehat{\mathbf{A}}^{\top}\widehat{\mathbf{A}}^{*} \in \mathbb{Z}_p^{k\times k}$ *is invertible if* $\widehat{\mathbf{A}}^{*}$ *forms a basis of* $\mathsf{Ker}\big((\mathbf{A}|\widetilde{\mathbf{A}})^{\top}\big)$.

For $Q \in \mathbb{N}$, we recall the Q-fold $\mathcal{U}_{\ell,k}$-MDDH assumption [11] as follows. One may view it as Q independent instances of the basic $\mathcal{U}_{\ell,k}$-MDDH problem.

Assumption 2 (Q-fold $\mathcal{U}_{\ell,k}$-MDDH [11]) *Let* $\mathcal{U}_{\ell,k}$ *be the uniform matrix distribution and* $s \in \{1, 2, T\}$*. For any p.p.t. adversary* $\mathcal{A}$ *against* GrpGen*, the following advantage function is negligible in* λ*.*

$$\mathsf{Adv}^{\mathcal{U}_{\ell,k}}_{\mathcal{A},Q}(\lambda) = |\Pr[\mathcal{A}(\mathcal{G}, [\mathbf{A}]_s, [\mathbf{AU}]_s) = 1] - \Pr[\mathcal{A}(\mathcal{G}, [\mathbf{A}]_s, [\mathbf{V}]_s) = 1]|$$

where $\mathcal{G} \leftarrow \mathsf{GrpGen}(1^{\lambda})$*,* $\mathbf{A} \leftarrow \mathcal{U}_{\ell,k}$*,* $\mathbf{U} \leftarrow \mathbb{Z}_p^{k\times Q}$*,* $\mathbf{V} \leftarrow \mathbb{Z}_p^{\ell\times Q}$*.*

It would be direct to prove "$\mathcal{U}_{\ell,k}$-MDDH $\Rightarrow$ Q-fold $\mathcal{U}_{\ell,k}$-MDDH" with a security loss Q. The *Random Self-reducibility Lemma* by Escala *et al.* [11] (see below) provided us with a tighter reduction, the security loss solely depends on the property of matrix $\mathbf{A}$ instead of Q. Namely one can deal with *unbounded* number of instances simultaneously with *constant* security loss for a fixed $\mathbf{A}$.

Lemma 4 (Random Self-reducibility [11]). *Assume* $Q > \ell - k$*. For any uniform matrix distribution* $\mathcal{U}_{\ell,k}$ *and any p.p.t. adversary* $\mathcal{A}$*, there exists an adversary* $\mathcal{B}$ *such that*

$$\mathsf{Adv}^{\mathcal{U}_{\ell,k}}_{\mathcal{A},Q}(\lambda) \leqslant (\ell - k)\cdot \mathsf{Adv}^{\mathcal{U}_{\ell,k}}_{\mathcal{B}}(\lambda) + 1/(p-1)$$

and $\mathsf{T}(\mathcal{B}) \approx \mathsf{T}(\mathcal{A}) + \ell^2 k \cdot \mathsf{poly}(\lambda)$ *where* $\mathsf{poly}(\lambda)$ *is independent of* $\mathsf{T}(\mathcal{A})$*.*

2.2 Identity Based Encryption

Algorithms. An *Identity Based Encryption* (IBE) in the multi-instance setting [3, 18, 14] consists of five p.p.t. algorithms:

- $\mathsf{Param}(1^{\lambda}, \textsc{sys}) \rightarrow \textsc{gp}$. The *parameter generation algorithm* takes as input a security parameter $\lambda \in \mathbb{Z}^{+}$ and a system-level parameter $\textsc{sys}$, and outputs a global parameter $\textsc{gp}$.
- $\mathsf{Setup}(\textsc{gp}) \rightarrow (\textsc{mpk}, \textsc{msk})$. The *setup algorithm* takes as input a global parameter $\textsc{gp}$, and outputs a master public/secret key pair $(\textsc{mpk}, \textsc{msk})$.

- $\mathsf{KeyGen}(\textsc{mpk}, \textsc{msk}, \textsc{id}) \to \textsc{sk}_{\textsc{id}}$. The *key generation algorithm* takes as input a master public key $\textsc{mpk}$, a master secret key $\textsc{msk}$ and an identity $\textsc{id}$, and outputs a secret key $\textsc{sk}_{\textsc{id}}$.
- $\mathsf{Enc}(\textsc{mpk}, \textsc{id}, \textsc{m}) \to \textsc{ct}_{\textsc{id}}$. The *encryption algorithm* takes as input a master public key $\textsc{mpk}$, an identity $\textsc{id}$ and a message $\textsc{m}$, outputs a ciphertext $\textsc{ct}_{\textsc{id}}$.
- $\mathsf{Dec}(\textsc{mpk}, \textsc{sk}, \textsc{ct}) \to \textsc{m}$. The *decryption algorithm* takes as input a master public key $\textsc{mpk}$, a secret key $\textsc{sk}$ and a ciphertext $\textsc{ct}$, outputs message $\textsc{m}$ or $\perp$.

If the IBE scheme in question is in the classical single-instance setting, we may merge the first two algorithms into a single Setup algorithm for clarity. The merged Setup algorithm takes 1^λ and $\textsc{sys}$ as inputs and creates a master public/secret key pair $(\textsc{mpk}, \textsc{msk})$.

Correctness. For any parameter $\lambda \in \mathbb{N}$, any $\textsc{sys}$, any $\textsc{gp} \in [\mathsf{Param}(1^\lambda, \textsc{sys})]$, any $(\textsc{mpk}, \textsc{msk}) \in [\mathsf{Setup}(\textsc{gp})]$, any identity $\textsc{id}$ and any message $\textsc{m}$, it holds that

$$\Pr\left[\mathsf{Dec}(\textsc{mpk}, \textsc{sk}, \textsc{ct}) = \textsc{m} \;\middle|\; \begin{array}{c} \textsc{sk} \leftarrow \mathsf{KeyGen}(\textsc{mpk}, \textsc{msk}, \textsc{id}) \\ \textsc{ct} \leftarrow \mathsf{Enc}(\textsc{mpk}, \textsc{id}, \textsc{m}) \end{array}\right] \geqslant 1 - 2^{-\Omega(\lambda)}.$$

Security Definition. We investigate both ciphertext indistinguishability and anonymity under chosen identity and plaintext attacks in the multi-instance, multi-ciphertext setting. We define the advantage function

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IBE}}(\lambda) = \left|\Pr\left[\beta = \beta' \;\middle|\; \begin{array}{c} \mu \leftarrow \mathcal{A}(),\ \textsc{gp} \leftarrow \mathsf{Param}(1^\lambda, \textsc{sys}),\ \beta \leftarrow \{0,1\} \\ (\textsc{mpk}_1, \textsc{msk}_1), \ldots, (\textsc{mpk}_\mu, \textsc{msk}_\mu) \leftarrow \mathsf{Setup}(\textsc{gp}) \\ \beta' \leftarrow \mathcal{A}^{\mathsf{O}_\beta^{\mathsf{Enc}}, \mathsf{O}^{\mathsf{KeyGen}}}(\textsc{mpk}_1, \ldots, \textsc{mpk}_\mu) \end{array}\right] - \frac{1}{2}\right|$$

where oracles $\mathsf{O}_\beta^{\mathsf{Enc}}$ and $\mathsf{O}^{\mathsf{KeyGen}}$ work as follows

- $\mathsf{O}_\beta^{\mathsf{Enc}}$: Given $(\iota_0^*, \textsc{id}_0^*, \iota_1^*, \textsc{id}_1^*, \textsc{m}_0^*, \textsc{m}_1^*)$, return $\mathsf{Enc}(\textsc{mpk}_{\iota_\beta^*}, \textsc{id}_\beta^*, \textsc{m}_\beta^*)$ and update $\mathcal{Q}_C = \mathcal{Q}_C \cup \{(\iota_0^*, \textsc{id}_0^*), (\iota_1^*, \textsc{id}_1^*)\}$.
- $\mathsf{O}^{\mathsf{KeyGen}}$: Given $(\iota, \textsc{id})$, return $\mathsf{KeyGen}(\textsc{mpk}_\iota, \textsc{msk}_\iota, \textsc{id})$ and update $\mathcal{Q}_K = \mathcal{Q}_K \cup \{(\iota, \textsc{id})\}$.

An identity based encryption scheme is *adaptively secure* and *anonymous* in the multi-instance, multi-ciphertext setting if for all p.p.t. adversary $\mathcal{A}$ the advantage function $\mathsf{Adv}_{\mathcal{A}}^{\mathsf{IBE}}(\lambda)$ is negligible in λ and $\mathcal{Q}_K \cap \mathcal{Q}_C = \emptyset$.

As a special case, the adaptive security and anonymity in the single-instance, single-ciphertext setting can be derived by setting two restrictions: (1) There is only one master public/secret key pair, i.e., we set $\mu = 1$ and all $\iota_0^*, \iota_1^*, \iota$ submitted to oracles are restricted to be 1. (2) There is only one challenge ciphertext, i.e., $\mathcal{A}$ can send only one query to oracle $\mathsf{O}_\beta^{\mathsf{Enc}}$.

3 A Technical Overview

3.1 Revisiting BKP

A Short Overview of BKP. Let $(G_1, G_2, G_T, p, e, g_1, g_2) \leftarrow \mathsf{GrpGen}(1^\lambda)$, let's review BKP, i.e., $\mathsf{IBE}[\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k], \mathcal{D}_k]$ in [4], which is derived from the affine

MAC based on Naor-Reingold PRF. The affine MAC can be described as follows.

$$\boxed{\begin{array}{lll} \textsc{sk}_{\mathsf{MAC}} & : & \mathbf{x}_{1,0},\ \mathbf{x}_{1,1},\ \ldots,\ \mathbf{x}_{n,0},\ \mathbf{x}_{n,1},\ x \\ \textsc{tag}_m & : & [\mathbf{t}]_2,\quad \big[\sum_{i=1}^n \mathbf{x}_{i,m[i]}^\top \mathbf{t} + x\big]_2 \end{array}}$$

Here $\mathbf{x}_{i,b} \leftarrow \mathbb{Z}_p^k$ for $(i,b) \in [n] \times \{0,1\}$ and $x \leftarrow \mathbb{Z}_p$, random coin $\mathbf{t} \in \mathbb{Z}_p^k$ is uniformly sampled for each tag and $m[i]$ represents the ith bit of message $m \in \{0,1\}^n$. It's beneficial to define *randomized verification key* for m^* as

$$\textsc{vk}_{m^*} \quad : \quad [h]_1, \quad \big[h \cdot \sum_{i=1}^n \mathbf{x}_{i,m^*[i]}\big]_1, \quad [h \cdot x]_T$$

where $h \leftarrow \mathbb{Z}_p$. Blazy *et al.* can prove that a verification key for m^* is pseudorandom for any p.p.t adversary holding tags for $m_1, \ldots, m_q \neq m^*$ under k-Lin assumption with $\mathcal{O}(n)$ security loss.

In a nutshell, the IBE scheme is obtained as follows: master secret key $\textsc{msk}$ is $\textsc{sk}_{\mathsf{MAC}}$; master public key $\textsc{mpk}$ consists of perfectly hiding commitments to $\textsc{sk}_{\mathsf{MAC}}$; a secret key $\textsc{sk}$ for $\textsc{id} \in \{0,1\}^n$ is composed of a tag $\textsc{tag}$ for $\textsc{id}$ and a Groth-Sahai NIZK proof [15] showing that $\textsc{tag}$ is correct under $\textsc{sk}_{\mathsf{MAC}}$; a ciphertext under $\textsc{id}$ and decryption algorithm are derived from verification method of the NIZK proof system. A more detailed description is given below.

$$\boxed{\begin{array}{llll} \textsc{mpk} & : & [\mathbf{A}]_1, [\mathbf{Z}_{1,0}]_1, [\mathbf{Z}_{1,1}]_1, \ldots, [\mathbf{Z}_{n,0}]_1, [\mathbf{Z}_{n,1}]_1, [\mathbf{z}]_1 & (\text{commitment to } \textsc{sk}_{\mathsf{MAC}}) \\ \textsc{sk}_{\textsc{id}} & : & [\mathbf{k}_0]_2,\ [k_1]_2 = \big[\sum_{i=1}^n \mathbf{x}_{i,\textsc{id}[i]}^\top \mathbf{k}_0 + x\big]_2 & (\text{MAC tag } \textsc{tag} \text{ for } \textsc{id}) \\ & & [\mathbf{k}_2]_2 = \big[\sum_{i=1}^n \mathbf{Y}_{i,\textsc{id}[i]}^\top \mathbf{k}_0 + \mathbf{y}^\top\big]_2 & (\text{proving validity of } \textsc{tag}) \\ \textsc{ct}_{\textsc{id}} & : & [\mathbf{A}\mathbf{s}]_1, \quad \big[\sum_{i=1}^n \mathbf{Z}_{i,\textsc{id}[i]}\mathbf{s}\big]_1, \quad [\mathbf{z}\mathbf{s}]_T \cdot \mathrm{M} & \end{array}}$$

Here $\mathbf{A} \leftarrow \mathcal{D}_k$ is commitment key, $\mathbf{Z}_{i,b} = (\mathbf{Y}_{i,b}|\mathbf{x}_{i,b})\mathbf{A}$ is a commitment to $\mathbf{x}_{i,b}$ with random coin $\mathbf{Y}_{i,b} \leftarrow \mathbb{Z}_q^{k\times k}$ for $(i,b) \in [\ell] \times \{0,1\}$, and $\mathbf{z} = (\mathbf{y}|x)\mathbf{A}$ is a commitment to x with random coin $\mathbf{y} \leftarrow \mathbb{Z}_q^{1\times k}$. To prove the security of BKP, one first transform the challenge ciphertext $\textsc{ct}_{\textsc{id}^*}$ into the form

$$[\mathbf{A}\mathbf{s} + \boxed{h} \cdot \mathbf{e}_{k+1}]_1,\ \big[\sum_{i=1}^n \mathbf{Z}_{i,\textsc{id}^*[i]}\mathbf{s} + \boxed{h \cdot \sum_{i=1}^n \mathbf{x}_{i,\textsc{id}^*[i]}}\big]_1,\ [\mathbf{z}\mathbf{s} + \boxed{h \cdot x}]_T \cdot \mathrm{M}$$

in which the boxed terms in fact form a verification key of $\textsc{id}^*$. Then we may rewrite the proof part $[\mathbf{k}_2]_2$ of $\textsc{sk}_{\textsc{id}}$ as

$$\mathbf{k}_2 = \overline{\mathbf{A}}^* \cdot \big(\sum_{i=1}^n \mathbf{Z}_{i,\textsc{id}[i]}^\top \mathbf{k}_0 + \mathbf{z}^\top - k_1 \underline{\mathbf{A}}^\top\big).$$

Here we use the following relation

$$\begin{aligned} \mathbf{Z}_{i,b} = (\mathbf{Y}_{i,b}|\mathbf{x}_{i,b})\mathbf{A} \ &\Leftrightarrow\ \mathbf{Y}_{i,b} = \mathbf{Z}_{i,b}\overline{\mathbf{A}}^{-1} - \mathbf{x}_{i,b}\underline{\mathbf{A}}\overline{\mathbf{A}}^{-1}, \quad (i,b) \in [n] \times \{0,1\} \\ \mathbf{z} = (\mathbf{y}|x)\mathbf{A} \ &\Leftrightarrow\ \mathbf{y} = \mathbf{z}\overline{\mathbf{A}}^{-1} - x\underline{\mathbf{A}}\overline{\mathbf{A}}^{-1}. \end{aligned}$$

From the standpoint of NIZK proof system, we have replaced the real proof with a *simulated* proof. An observation is that we do not need $\mathbf{Y}_{i,b}$ (resp. $\mathbf{y}$) and $\mathbf{Z}_{i,b}$ (resp. $\mathbf{z}$) and $\mathbf{x}_{i,b}$ (resp. x) are distributed *independently* by the property of perfectly hiding commitment. In this case we can reduce the adaptive security and anonymity of BKP to the property of underlying affine MAC we just mentioned.

BKP in the Dual-system Lens. Although Blazy *et al.*'s proof [4] is in the framework of dual system encryption [34, 9], from their exposition, it's seemingly difficult to identify normal space and semi-functional space, which may guide us to a better understanding and has been formulated via dual system group (DSG) [10] and NDSG [9] (as well as ENDSG [18, 14]). Fortunately, ciphertexts and keys used in the proof (c.f. paragraph **A Short Overview of BKP**) give us the following (informal) observations:

- the commitments $\mathbf{Z}_{i,b}$ and $\mathbf{z}$ lie in the normal space;
- the values being committed to, $\mathbf{x}_{i,b}$ and x, lie in the semi-functional space.

Now we try to put the structure into the real system instead of in the proof. For simplicity, we ignore the master secret (i.e., $\mathbf{z}$, $\mathbf{y}$ and x). From the relation in the previous paragraph, we readily have the following representation:

$$\begin{pmatrix} \mathbf{Y}_{i,b}^\top \\ \mathbf{x}_{i,b}^\top \end{pmatrix} = \begin{pmatrix} \overline{\mathbf{A}}^* & -\overline{\mathbf{A}}^* \underline{\mathbf{A}}^\top \\ \mathbf{0}_{1\times k} & 1 \end{pmatrix} \begin{pmatrix} \mathbf{Z}_{i,b}^\top \\ \mathbf{x}_{i,b}^\top \end{pmatrix}, \quad \forall\ (i,b) \in [n] \times \{0,1\}.$$

We find that the transformation matrix above actually forms the dual basis of $(\mathbf{A}|\mathbf{e}_{k+1}) = \left(\begin{smallmatrix} \overline{\mathbf{A}} & \mathbf{0}_k \\ \underline{\mathbf{A}} & 1 \end{smallmatrix}\right)$. A simple substitution results in secret keys (without master secret) in the following form:

$$[\mathbf{k}_0]_2, \qquad \begin{bmatrix} \mathbf{k}_2 \\ k_1 \end{bmatrix}_2 = \left[\sum_{i=1}^{n} (\mathbf{A}|\mathbf{e}_{k+1})^* \begin{pmatrix} \mathbf{Z}_{i,\mathrm{ID}[i]}^\top \\ \mathbf{x}_{i,\mathrm{ID}[i]}^\top \end{pmatrix} \mathbf{k}_0 \right]_2 .$$

As we have observed, $\mathbf{Y}_{i,b}$ is not needed when creating secret keys and ciphertexts *in the real system* and $\mathbf{Z}_{i,b}$ and $\mathbf{x}_{i,b}$ are distributed independently. Therefore we may sample them *directly* instead of through $\mathbf{Y}_{i,b}$. In particular, we sample $\mathbf{W}_{i,b} \leftarrow \mathbb{Z}_p^{k\times(k+1)}$ for all $(i,b) \in [n] \times \{0,1\}$ and define $\mathbf{Z}_{i,b}$ and $\mathbf{x}_{i,b}$ such that

$$\mathbf{W}_{i,b}^\top = (\mathbf{A}|\mathbf{e}_{k+1})^* \begin{pmatrix} \mathbf{Z}_{i,b}^\top \\ \mathbf{x}_{i,b}^\top \end{pmatrix}$$

or equivalently define $\mathbf{Z}_{i,b} = \mathbf{W}_{i,b}\mathbf{A}$ and $\mathbf{x}_{i,b} = \mathbf{W}_{i,b}\mathbf{e}_{k+1}$. This allows us to simplify BKP (without considering master secret key and payload) as follows:

$$\boxed{\begin{array}{lll} \mathrm{MPK} & : [\mathbf{A}]_1,\ [\mathbf{W}_{1,0}\mathbf{A}]_1, [\mathbf{W}_{1,1}\mathbf{A}]_1,\ \ldots,\ [\mathbf{W}_{n,0}\mathbf{A}]_1,\ [\mathbf{W}_{n,1}\mathbf{A}]_1 & \\ \mathrm{CT}_{\mathrm{ID}} & : [\mathbf{A}\mathbf{s}]_1,\ \left[\sum_{i=1}^{n} \mathbf{W}_{i,\mathrm{ID}[i]}\mathbf{A}\mathbf{s}\right]_1 \quad \in G_1^{k+1} \times G_1^{k} & \\ \mathrm{SK}_{\mathrm{ID}} & : [\mathbf{k}_0]_2,\ \left[\sum_{i=1}^{n} \mathbf{W}_{i,\mathrm{ID}[i]}^\top \mathbf{k}_0\right]_2 \quad \in G_2^{k} \times G_2^{k+1} & \end{array}}$$

which is surprisingly close to Chen *et al.*'s structure [8].

Remark 1. The structure presented here also appeared in a quasi-adaptive NIZK (QA-NIZK) recently proposed by Gay *et al.* [12]. They obtained this structure from their pairing-free designated-verifier QA-NIZK. In fact, we can alternatively derive their QA-NIZK from the basic QA-NIZK with no support to simulation soundness in [20] (see their Introduction) and a randomized PRF underlying the above structure (following the semi-general method of reaching unbounded simulation soundness in [20]).

3.2 Technical Result 1: Generalizing NDSG

The similarity between Chen *et al.*'s structure [8] and simplified BKP suggests that one may study simplified BKP under the framework of NDSG [9]. However Chen and Wee's NDSG [9] is not sufficient for our purpose and a series of adjustments are seemingly necessary.

Informally, NDSG defines an abstract bilinear group $(\mathbb{G}, \mathbb{H}, \mathbb{G}_T, e)$ equipped with a collection of algorithms sampling group elements. In the generic construction of IBE, a ciphertext (excluding the payload) consists of elements from $\mathbb{G}$ while a secret key is composed of elements in $\mathbb{H}$. However both ciphertexts and keys in the above observation involve elements from two distinct groups, i.e., G_1^{k+1} and G_1^k for CT_{ID} and G_2^k and G_2^{k+1} for SK_{ID}. We generalize Chen and Wee's NDSG [9] in the following aspects:

- replace $\mathbb{G}$ with $\mathbb{G}_0$ and $\mathbb{G}$;
- replace $\mathbb{H}$ with $\mathbb{H}_0$ and $\mathbb{H}$;
- replace e with e and e_0 which map $\mathbb{G} \times \mathbb{H}_0$ and $\mathbb{G}_0 \times \mathbb{H}$ to $\mathbb{G}_T$, respectively.

The first two points are straightforward while the last one is motivated by the decryption procedure where only two vectors of the same dimensions, i.e., either k or $k + 1$ dimension, can be paired together and the results should lie in $\mathbb{G}_T$ in both case. Of course, more fine-tunings are required for other portions of NDSG (including making SampH private as in [14], see Section 4 for more detail).

Furthermore, following Chen *et al.* [8], we also upgrade NDSG (with all above generalization) to support *weak* anonymity. In particular, we define an additional requirement, called $\mathbb{G}$-uniformity, which is a combination of $\mathbb{H}$-hiding and a weakened $\mathbb{G}$-uniformity in [8]. This allows us to implement its computational version (we will discuss it later) in a tighter fashion.

It's not hard to verify that our generalized NDSG implies an almost-tightly secure IBE in the SISC setting with weaker anonymity [3]. Motivated by our simplified BKP, we can provide a prime-order instantiation of our generalized NDSG. All computational requirements (i.e., left-subgroup and nested-hiding indistinguishability) are proved under the k-Lin assumption based on [8, 4].

3.3 Technical Result 2: Towards MIMC Setting

All previous informal discussion and formal treatment are preparations for moving from SISC towards MIMC settings. Having a generalized NDSG with a prime-order instantiation, we can now apply the extension technique proposed in [18, 14]. This finally results in a *generalized* extended NDSG (ENDSG) [18, 14] and its prime-order instantiation, which immediately gives us an almost-tightly secure and *weakly* anonymous IBE in the MIMC setting, i.e., our main result (c.f. Section 1.2 and Section 6).

Apart from regular extension procedure [18, 14] introducing new algorithms and requirements, we also update the $\mathbb{G}$-uniformity (in our generalized NDSG) to its computational version. It's direct to check that the computational $\mathbb{G}$-uniformity gives to our generalized ENDSG the power of reaching *weak* anonymity [3] in the MIMC setting.

The prime-order instantiation of generalized ENDSG and its proofs are obtained from those for the generalized NDSG following the extension strategy by Gong *et al.* [14] and its recent refinement from Gay *et al.* [12]. In particular, the most important extensions must be:

- We let the bases of normal, $\wedge$-semi-functional, and $\sim$-semi-functional space be $\mathbf{A}$, $\widehat{\mathbf{A}}$, and $\widetilde{\mathbf{A}}$, respectively, all of which are sampled from uniform matrix distribution over $\mathbb{Z}_p^{3k\times k}$. The size of matrix $\mathbf{W}$ randomizing bases are extended from $k \times (k+1)$ to $k \times 3k$ accordingly.
- Random functions $\widehat{\mathsf{RF}}_i$ and $\widetilde{\mathsf{RF}}_i$ map an binary string (say, the i-bit prefix of an identity) to a random element in $\mathsf{Span}(\widehat{\mathbf{A}}^*)$ and $\mathsf{Span}(\widetilde{\mathbf{A}}^*)$, respectively. Here we let $\widehat{\mathbf{A}}^*$ (resp. $\widetilde{\mathbf{A}}^*$) be a basis of $\mathsf{Ker}\big((\mathbf{A}|\widetilde{\mathbf{A}})^\top\big)$ (resp. $\mathsf{Ker}\big((\mathbf{A}|\widehat{\mathbf{A}})^\top\big)$) following Gay *et al.*'s method [12].

This prime-order instantiation derives an IBE (i.e., our main result) with ciphertexts of size $(3k+\boxed{k})|G_1| = 4k|G_1|$ and secret keys of size $(\boxed{k}+3k)|G_2| = 4k|G_2|$. We highlight that, with the above extension,

- all $\mathbf{W}_{i,b}\mathbf{A}$ are still of size $k \times k$ (see the first boxed term);
- the random coin $\mathbf{r}$ for key is still k dimensional (see the second boxed term).

Namely *not all components in ciphertexts and secret keys swell in our extension procedure* which seemingly benefits from Blazy *et al.*'s structure [4]. More importantly, we gain this feature without relying on the technique presented in [14] which compresses both two semi-functional spaces and thus has to turn to a non-standard assumption.

3.4 Discussion and Perspective

Besides acting as the cornerstone of Technical Result 2, we believe Technical Result 1 may be of independent interest due to its clean description and proofs. For instance, it allows us to explain why BKP can be more efficient than CW, which is not quite obvious before. As a matter of fact, through Technical Result 1, we can compare CW with BKP in the same framework and perceive two differences between them which make BKP more efficient.

Firstly, the secret keys in CW contain a structure supporting *parameter-hiding* which is not found in BKP's secret keys. It is previously used to achieve *right subgroup indistinguishability* in Chen and Wee's prime-order instantiation of DSG [10] but is actually not needed when proving almost-tight adaptive security using Chen and Wee's technique [9].

Secondly, the proof of *nested-hiding indistinguishability* is stronger such that corresponding structure on the key side in BKP are much simpler than in CW. We highlight this point in our proof (in Section 4.3) via a lemma (Lemma 5) extracted from Blazy *et al.*'s proof. We specially describe it in the same flavor as Chen and Wee's *Many Tuple Lemma* [9]. One can think of it as a stronger version of *Many Tuple Lemma* [9] since it just involves a secret *vector* instead of a *matrix* which costs less space to hide.

4 Blazy-Kiltz-Pan Almost-tightly Secure IBE, Revisited

4.1 Generalized Nested Dual System Group

Keeping our informal discussion in Section 3 in mind, we generalize the notion of nested dual system group (NDSG) [9] in this section. The formal definition is followed by remarks illustrating main differences with the original one.

Algorithms. Our generalized NDSG consists of five p.p.t. algorithms as follows:

- $\mathsf{SampP}(1^\lambda, n)$: Output $(\textsc{pp}, \textsc{sp})$ where:
  - $\textsc{pp}$ contains group $(\mathbb{G}_0, \mathbb{G}, \mathbb{H}_0, \mathbb{H}, \mathbb{G}_T)$ and admissible bilinear maps

$$e_0 : \mathbb{G}_0 \times \mathbb{H} \to \mathbb{G}_T \quad \text{and} \quad e : \mathbb{G} \times \mathbb{H}_0 \to \mathbb{G}_T,$$

    an efficient linear map μ defined on $\mathbb{H}$, and public parameters for SampG;
  - $\textsc{sp}$ contains $h^* \in \mathbb{H}$ and secret parameters for SampH, $\widehat{\mathsf{SampG}}$.
- SampGT: $\mathrm{Im}(\mu) \to \mathbb{G}_T$.
- $\mathsf{SampG}(\textsc{pp})$: Output $\mathbf{g} = (g_0;\ g_1,\ \ldots,\ g_n) \in \mathbb{G}_0 \times \mathbb{G}^n$.
- $\mathsf{SampH}(\textsc{pp}, \textsc{sp})$: Output $\mathbf{h} = (h_0;\ h_1,\ \ldots,\ h_n) \in \mathbb{H}_0 \times \mathbb{H}^n$.
- $\widehat{\mathsf{SampG}}(\textsc{pp}, \textsc{sp})$: Output $\widehat{\mathbf{g}} = (\widehat{g}_0;\ \widehat{g}_1,\ \ldots,\ \widehat{g}_n) \in \mathbb{G}_0 \times \mathbb{G}^n$.

We employ SampG_0 (resp., $\widehat{\mathsf{SampG}}_0$) to indicate the first element $g_0 \in \mathbb{G}_0$ (resp., $\widehat{g}_0 \in \mathbb{G}_0$) in the output of SampG (resp., $\widehat{\mathsf{SampG}}$). We simply view the outputs of the last three algorithms as vectors but use a semicolon to emphasize the first element and all remaining ones belong to distinct groups.

Correctness. For all $\lambda, n \in \mathbb{Z}^+$ and all $(\textsc{pp}, \textsc{sp}) \in [\mathsf{SampP}(1^\lambda, n)]$, we require:

(projective) For all $h \in \mathbb{H}$ and coin s, $\mathsf{SampGT}(\mu(h); s) = e_0(\mathsf{SampG}_0(\textsc{pp}; s), h)$.
(associative) For all $(g_0;\ g_1,\ \ldots,\ g_n) \in [\mathsf{SampG}(\textsc{pp})]$ and $(h_0;\ h_1,\ \ldots,\ h_n) \in [\mathsf{SampH}(\textsc{pp}, \textsc{sp})]$, $e_0(g_0, h_i) = e(g_i, h_0)$ for all $i \in [n]$.

Security. For all $\lambda, n \in \mathbb{Z}^+$ and $(\textsc{pp}, \textsc{sp}) \leftarrow \mathsf{SampP}(1^\lambda, n)$, we require:

(orthogonality) $\mu(h^*) = 1$.
(non-degeneracy) With overwhelming probability when $\widehat{g}_0 \leftarrow \widehat{\mathsf{SampG}}_0(\textsc{pp}, \textsc{sp})$, the value $e_0(\widehat{g}_0, h^*)^\alpha$ is uniformly distributed over $\mathbb{G}_T$ where $\alpha \leftarrow \mathbb{Z}_{\mathsf{ord}(\mathbb{H})}$.
($\mathbb{H}$-subgroup) The output of $\mathsf{SampH}(\textsc{pp}, \textsc{sp})$ is uniformly distributed over some subgroup of $\mathbb{H}_0 \times \mathbb{H}^n$.
(left subgroup indistinguishability) For any p.p.t. adversary $\mathcal{A}$, the following advantage function is negligible in λ.

$$\mathsf{Adv}^{\mathrm{LS}}_{\mathcal{A}}(\lambda, q) = \left|\Pr[\mathcal{A}(\textsc{pp}, \{\mathbf{h}_j\}_{j\in[q]}, \boxed{\mathbf{g}}) = 1] - \Pr[\mathcal{A}(\textsc{pp}, \{\mathbf{h}_j\}_{j\in[q]}, \boxed{\mathbf{g} \cdot \widehat{\mathbf{g}}}) = 1]\right|$$

where $\mathbf{g} \leftarrow \mathsf{SampG}(\textsc{pp})$, $\widehat{\mathbf{g}} \leftarrow \widehat{\mathsf{SampG}}(\textsc{pp}, \textsc{sp})$, $\mathbf{h}_j \leftarrow \mathsf{SampH}(\textsc{pp}, \textsc{sp})$.

(nested-hiding indistinguishability) For all $\eta \in [n]$ and any p.p.t. adversary $\mathcal{A}$, the following advantage function is negligible in λ.

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{NH}(\eta)}(\lambda, q) = |\Pr[\mathcal{A}(D, T_0) = 1] - \Pr[\mathcal{A}(D, T_1) = 1]|,$$

where $D = \big(\textsc{pp}, h^*, \widehat{\mathbf{g}}_{-\eta}, \{\mathbf{h}'_j\}_{j\in[q]}\big)$,

$$T_0 = \big\{\mathbf{h}_j\big\}_{j\in[q]}, \qquad T_1 = \big\{\mathbf{h}_j \cdot \boxed{(1_{\mathbb{H}_0}; (h^*)^{\gamma_j \mathbf{e}_\eta})}\big\}_{j\in[q]}$$

and $\widehat{\mathbf{g}} \leftarrow \widehat{\mathsf{SampG}}(\textsc{pp}, \textsc{sp})$, $\mathbf{h}_j, \mathbf{h}'_j \leftarrow \mathsf{SampH}(\textsc{pp}, \textsc{sp})$, $\gamma_j \leftarrow \mathbb{Z}_{\mathsf{ord}(\mathbb{H})}$, $\widehat{\mathbf{g}}_{-\eta}$ refers to $(\widehat{g}_0; \widehat{g}_1, \ldots, \widehat{g}_{\eta-1}, \widehat{g}_{\eta+1}, \ldots, \widehat{g}_n)$, $\mathbf{e}_\eta$ is an n-dimension identity vector with a 1 on the ηth position. We can define $\mathsf{Adv}_{\mathcal{A}}^{\mathrm{NH}}(\lambda, q) = \max_{\eta\in[n]} \big\{\mathsf{Adv}_{\mathcal{A}}^{\mathrm{NH}(\eta)}(\lambda, q)\big\}$.

($\mathbb{G}$-uniformity) The statistical distance between the following two distributions is bounded by $2^{-\Omega(\lambda)}$.

$$\Big\{\textsc{pp}, h^*, \big\{\mathbf{h}_j \cdot (1_{\mathbb{H}_0}; (h^*)^{\widehat{\mathbf{v}}_j})\big\}_{j\in[q]}, \boxed{\mathbf{g} \cdot \widehat{\mathbf{g}}}\Big\} \quad \text{and}$$
$$\Big\{\textsc{pp}, h^*, \big\{\mathbf{h}_j \cdot (1_{\mathbb{H}_0}; (h^*)^{\widehat{\mathbf{v}}_j})\big\}_{j\in[q]}, \boxed{\mathbf{g} \cdot \widehat{\mathbf{g}} \cdot (1_{\mathbb{G}_0}; (g')^{\mathbf{1}_n})}\Big\}$$

where $\mathbf{h}_j \leftarrow \mathsf{SampH}(\textsc{pp}, \textsc{sp})$, $\mathbf{g} \leftarrow \mathsf{SampG}(\textsc{pp})$, $\widehat{\mathbf{g}} \leftarrow \widehat{\mathsf{SampG}}(\textsc{pp}, \textsc{sp})$, $\widehat{\mathbf{v}}_j \leftarrow \mathbb{Z}^n_{\mathsf{ord}(\mathbb{H})}$, $g' \leftarrow \mathbb{G}$, $\mathbf{1}_n$ is a vector of n 1's.

One can construct an IBE scheme from generalized NDSG following Chen and Wee's generic construction [9]. The master public/secret key pair is

$$\textsc{mpk} = (\textsc{pp}, \mu(\textsc{msk}_0)) \quad \text{and} \quad \textsc{msk} = (\textsc{msk}_0, \textsc{sp}).$$

where $(\textsc{pp}, \textsc{sp}) \leftarrow \mathsf{SampP}(1^\lambda, 2n)$ and $\textsc{msk}_0 \leftarrow \mathbb{H}$. A secret key for $\textsc{id}$ is

$$\textsc{sk}_{\textsc{id}} = \big(K_0 = h_0,\ K_1 = \textsc{msk}_0 \cdot \textstyle\prod_{i\in[n]} h_{2i-\textsc{id}[i]}\big) \in \mathbb{H}_0 \times \mathbb{H}.$$

where $(h_0; h_1, \ldots, h_{2n}) \leftarrow \mathsf{SampH}(\textsc{pp}, \textsc{sp})$. A ciphertext for $\textsc{m}$ under $\textsc{id}$ is

$$\textsc{ct}_{\textsc{id}} = \big(C_0 = g_0,\ C_1 = \textstyle\prod_{i\in[n]} g_{2i-\textsc{id}[i]},\ C_2 = g'_T \cdot \textsc{m}\big) \in \mathbb{G}_0 \times \mathbb{G} \times \mathbb{G}_T.$$

where $(g_0; g_1, \ldots, g_{2n}) \leftarrow \mathsf{SampG}(\textsc{pp}; s)$ and $g'_T = \mathsf{SampGT}(\mu(\textsc{msk}_0); s)$ for random coin s. The message can be recovered by $\textsc{m} = C_2 \cdot e(C_1, K_0)/e_0(C_0, K_1)$.

Remark 2 (group structure). We generalized SampG, $\widehat{\mathsf{SampG}}$ and SampH such that elements they outputs may come from two different groups. Of course, the new groups $\mathbb{G}_0$ and $\mathbb{H}_0$ are generated via SampP and described in $\textsc{pp}$. Motivated by the decryption procedure (see the graph below), we require two bilinear maps e_0 and e, denoted by dash line and solid line, respectively, in the graph.

$$\begin{tikzcd}
\textsc{ct}_{\textsc{id}} : & C_0 \in \mathbb{G}_0 \arrow[dr, dash, dashed] & C_1 \in \mathbb{G} \arrow[dl, dash] & C_2 \in \mathbb{G}_T \\
\textsc{sk}_{\textsc{id}} : & K_0 \in \mathbb{H}_0 & K_1 \in \mathbb{H} &
\end{tikzcd}$$

It's worth noting that both maps share the same range $\mathbb{G}_T$, which helps us to preserve the *associative* property and thus the correctness of IBE scheme.

Remark 3 (private SampH*).* We make the algorithm SampH private as in [14]. One should run SampH with $\textsc{sp}$ besides $\textsc{pp}$. Therefore *left subgroup* and *nested-hiding indistinguishability* are modified accordingly [14] since adversary now cannot run SampH by itself.

Remark 4 ($\mathbb{G}$-uniformity and anonymity). The $\mathbb{G}$-uniformity property is used to achieve the anonymity. Our definition could be viewed as a direct combination of $\mathbb{H}$-hiding and $\mathbb{G}$-uniformity described by Chen *et al.* in [8] with a tiny relaxation. In particular, we require the last n elements in $\mathbf{g} \cdot \widehat{\mathbf{g}}$ to be hidden by *one* random element from $\mathbb{G}$ instead of n *i.i.d.* random elements in $\mathbb{G}$ as in [8]. One can check that our definition is sufficiently strong to prove the *weak* anonymity [3] (c.f. Section 2.2) of our generic IBE scheme.

4.2 A Prime-order Instantiation Motivated by BKP

We provide an instantiation of our generalized NDSG in the prime-order bilinear group. This formulates our (informal) observation in Section 3.1.

– $\mathsf{SampP}(1^\lambda, n)$: Run $\mathcal{G} = (G_1, G_2, G_T, p, e, g_1, g_2) \leftarrow \mathsf{GrpGen}(1^\lambda)$. Define

$$\mathbb{G}_0 = G_1^{k+1}, \quad \mathbb{G} = G_1^k, \quad \mathbb{H}_0 = G_2^k, \quad \mathbb{H} = G_2^{k+1}$$

and bilinear map e_0 and e are natural extensions of e (given in $\mathcal{G}$) to $(k+1)$-dim and k-dim, respectively. Sample $(\mathbf{A}, \mathbf{a}^\perp) \leftarrow \mathcal{D}_k$ and $\mathbf{b} \leftarrow \mathbb{Z}_p^{k+1}$. For each $\mathbf{k} \in \mathbb{Z}_p^{k+1}$, define $\mu : G_2^{k+1} \to G_T^k$ by

$$\mu([\mathbf{k}]_2) = e([\mathbf{A}]_1, [\mathbf{k}]_2) = [\mathbf{A}^\top \mathbf{k}]_T.$$

Let $h^* = [\mathbf{a}^\perp]_2 \in G_2^{k+1}$. Pick $\mathbf{W}_i \leftarrow \mathbb{Z}_p^{k \times (k+1)}$ for all $i \in [n]$ and output

$$\textsc{pp} = \big([\mathbf{A}]_1,\ [\mathbf{W}_1\mathbf{A}]_1,\ \ldots,\ [\mathbf{W}_n\mathbf{A}]_1\big), \quad \textsc{sp} = \big(\mathbf{a}^\perp,\ \mathbf{b},\ \mathbf{W}_1,\ \ldots,\ \mathbf{W}_n\big).$$

– $\mathsf{SampGT}([\mathbf{p}]_T)$: Sample $\mathbf{s} \leftarrow \mathbb{Z}_p^k$ and output $[\mathbf{s}^\top \mathbf{p}]_T \in G_T$ for $\mathbf{p} \in \mathbb{Z}_p^k$.

– $\mathsf{SampG}(\textsc{pp})$: Sample $\mathbf{s} \leftarrow \mathbb{Z}_p^k$ and output

$$\big([\mathbf{A}\mathbf{s}]_1;\ [\mathbf{W}_1\mathbf{A}\mathbf{s}]_1,\ \ldots,\ [\mathbf{W}_n\mathbf{A}\mathbf{s}]_1\big) \in G_1^{k+1} \times (G_1^k)^n.$$

– $\mathsf{SampH}(\textsc{pp}, \textsc{sp})$: Sample $\mathbf{r} \leftarrow \mathbb{Z}_p^k$ and output

$$\big([\mathbf{r}]_2;\ [\mathbf{W}_1^\top \mathbf{r}]_2,\ \ldots,\ [\mathbf{W}_n^\top \mathbf{r}]_2\big) \in G_2^k \times (G_2^{k+1})^n.$$

– $\widehat{\mathsf{SampG}}(\textsc{pp}, \textsc{sp})$: Sample $\widehat{s} \leftarrow \mathbb{Z}_p$ and output

$$\big([\mathbf{b}\widehat{s}]_1;\ [\mathbf{W}_1\mathbf{b}\widehat{s}]_1,\ \ldots,\ [\mathbf{W}_n\mathbf{b}\widehat{s}]_1\big) \in G_1^{k+1} \times (G_1^k)^n.$$

We only describe formal proof for *nested-hiding indistinguishability* for the lack of space. The remaining requirements can be proved following [8] and [12].

4.3 Nested-hiding Indistinguishability

We may rewrite the advantage function $\mathsf{Adv}^{\mathrm{NH}(\eta)}_{\mathcal{A}}(\lambda, q)$ using

$$\begin{aligned}
\textsc{pp} &= \big([\mathbf{A}]_1,\ [\mathbf{W}_1\mathbf{A}]_1,\ \ldots,\ [\mathbf{W}_n\mathbf{A}]_1\big);\\
h^* &= [\mathbf{a}^{\perp}]_2;\\
\widehat{\mathbf{g}} &= \big([\mathbf{b}\widehat{s}]_1;\ [\mathbf{W}_1\mathbf{b}\widehat{s}]_1, \ldots, [\mathbf{W}_n\mathbf{b}\widehat{s}]_1\big), \quad \widehat{s} \leftarrow \mathbb{Z}_p;\\
\mathbf{h}'_j &= \big([\mathbf{r}'_j]_2;\ [\mathbf{W}_1^{\top}\mathbf{r}'_j]_2,\ \ldots,\ [\mathbf{W}_n^{\top}\mathbf{r}'_j]_2\big), \quad \mathbf{r}'_j \leftarrow \mathbb{Z}_p^k
\end{aligned}$$

and the challenge term $\{\mathbf{h}_j \cdot (1_{\mathbb{H}_0}; (h^*)^{\gamma_j \mathbf{e}_\eta})\}$ may be written as

$$\big([\mathbf{r}_j]_2;\ [\mathbf{W}_1^{\top}\mathbf{r}_j]_2, \ldots, [\mathbf{W}_\eta^{\top}\mathbf{r}_j + \mathbf{a}^{\perp}\gamma_j]_2, \ldots, [\mathbf{W}_n^{\top}\mathbf{r}_j]_2\big), \quad \mathbf{r}_j \leftarrow \mathbb{Z}_p^k,$$

where either $\gamma_j \leftarrow \mathbb{Z}_p$ or $\gamma_j = 0$.

Before we proceed, we first prove a lemma implicitly used in Blazy *et al.*'s proof [4], which looks like the *Many Tuple Lemma* by Chen and Wee [9].

Lemma 5. *Given $Q \in \mathbb{N}$, group G of prime order p, $[\mathbf{M}] \in G^{(k+1)\times k}$ and $[\mathbf{T}] = [\mathbf{t}_1|\cdots|\mathbf{t}_Q] \in G^{(k+1)\times Q}$ (Here $[\cdot]$ is the implicit representation on G.) where either $\mathbf{t}_i \leftarrow \mathsf{Span}(\mathbf{M})$ or $\mathbf{t}_i \leftarrow \mathbb{Z}_p^{k+1}$, one can efficiently compute*

$$[\mathbf{Z}], \quad [\mathbf{v}\mathbf{Z}], \quad \{[\boldsymbol{\tau}_j], [\tau_j]\}_{j\in[Q]}$$

where $\mathbf{Z} \in \mathbb{Z}_p^{k\times k}$ is full-rank, $\mathbf{v} \in \mathbb{Z}_p^{1\times k}$ is a secret row vector, $\boldsymbol{\tau}_j \leftarrow \mathbb{Z}_p^k$, either $\tau_j = \mathbf{v}\boldsymbol{\tau}_j$ (when $\mathbf{t}_j \leftarrow \mathsf{Span}(\mathbf{M})$) or $\tau_j \leftarrow \mathbb{Z}_p$ (when $\mathbf{t}_j \leftarrow \mathbb{Z}_p^{k+1}$).

Proof. Given Q, G, $[\mathbf{M}]$, $[\mathbf{T}] = [\mathbf{t}_1|\cdots|\mathbf{t}_Q]$, the algorithm works as follows:

Programming $[\mathbf{Z}]$ and $[\mathbf{vZ}]$. Define $\mathbf{Z} = \overline{\mathbf{M}}$. Pick $\mathbf{m} = (m_1, \ldots, m_k, m_{k+1}) \leftarrow \mathbb{Z}_p^{1\times(k+1)}$ and implicitly define $\mathbf{v} \in \mathbb{Z}_p^{1\times k}$ such that

$$\mathbf{v}\mathbf{Z} = \mathbf{v}\overline{\mathbf{M}} = \mathbf{m}\mathbf{M}.$$

One can compute $[\mathbf{Z}]$ and $[\mathbf{vZ}]$ using $[\mathbf{M}]$ and $\mathbf{m}$.

Generating Q tuples. For all $j \in [Q]$, we compute

$$[\boldsymbol{\tau}_j] = [\overline{\mathbf{t}}_j] \ \text{ and } \ [\tau_j] = [\mathbf{m}\mathbf{t}_j].$$

Here $\overline{\mathbf{t}}_j$ indicates the first k entries of $\mathbf{t}_j$.

Observe that: if $\mathbf{t}_j = \mathbf{M}\mathbf{u}_j$ for some $\mathbf{u}_j \in \mathbb{Z}_p^k$, we have that $\boldsymbol{\tau}_j = \overline{\mathbf{M}}\mathbf{u}_j$ and $\tau_j = \mathbf{m}\mathbf{M}\mathbf{u}_j = \mathbf{v}\overline{\mathbf{M}}\mathbf{u}_j = \mathbf{v}\boldsymbol{\tau}_j$; if $\mathbf{t}_j \leftarrow \mathbb{Z}_p^{k+1}$, we can see that

$$\begin{pmatrix}\boldsymbol{\tau}_j\\ \tau_j\end{pmatrix} = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ m_1 & \cdots & m_k & m_{k+1}\end{pmatrix}\mathbf{t}_j$$

is uniformly distributed over $\mathbb{Z}_p^{k+1}$. This readily proves the lemma. □

We now prove the following lemma for all $\eta \in [n]$.

Lemma 6. *For any p.p.t. adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$ such that*

$$\mathsf{Adv}^{\mathrm{NH}(\eta)}_{\mathcal{A}}(\lambda, q) \leqslant \mathsf{Adv}^{\mathcal{D}_k}_{\mathcal{B},q}(\lambda)$$

where $\mathsf{T}(\mathcal{B}) \approx \mathsf{T}(\mathcal{A}) + k^2 \cdot q \cdot \mathsf{poly}(\lambda, n)$ and $\mathsf{poly}(\lambda, n)$ is independent of $\mathsf{T}(\mathcal{A})$.

Proof. Given $[\mathbf{M}]_2 \in G_2^{(k+1)\times k}$ and $[\mathbf{T}]_2 = [\mathbf{t}_1|\cdots|\mathbf{t}_q]_2 \in G_2^{(k+1)\times q}$ where $\mathbf{t}_j \leftarrow \mathsf{Span}(\mathbf{M})$ or $\mathbf{t}_j \leftarrow \mathbb{Z}_p^{k+1}$, $\mathcal{B}$ proceeds as follows:

Generating q tuples. We invoke the algorithm described in Lemma 5 on input $(q, G_2, [\mathbf{M}]_2, [\mathbf{T}]_2)$ and obtain $\big([\mathbf{Z}]_2,\ [\mathbf{v}\mathbf{Z}]_2,\ \big\{[\boldsymbol{\tau}_j]_2, [\tau_j]_2\big\}_{j\in[q]}\big)$.

Simulating pp and h^*. Sample $(\mathbf{A}, \mathbf{a}^\perp) \leftarrow \mathcal{D}_k$ and define $h^* = [\mathbf{a}^\perp]_2$. Sample $\mathbf{W}_i \leftarrow \mathbb{Z}_p^{k\times(k+1)}$ for all $i \in [n] \setminus \{\eta\}$. Pick $\bar{\mathbf{W}}_\eta \leftarrow \mathbb{Z}_p^{k\times(k+1)}$ and implicitly set

$$\mathbf{W}_\eta = \bar{\mathbf{W}}_\eta + \mathbf{v}^\top {\mathbf{a}^\perp}^\top.$$

Therefore we can simulate all entries in PP with the observation

$$\mathbf{W}_\eta \mathbf{A} = \big(\bar{\mathbf{W}}_\eta + \mathbf{v}^\top {\mathbf{a}^\perp}^\top\big)\mathbf{A} = \bar{\mathbf{W}}_\eta \mathbf{A},$$

where the secret vector $\mathbf{v}$ has been eliminated by the fact $\mathbf{A}^\top \mathbf{a}^\perp = \mathbf{0}$.

Simulating $\widehat{\mathbf{g}}_{-\eta}$. Sample $\mathbf{b} \leftarrow \mathbb{Z}_p^{k+1}$. We can directly simulate $\widehat{\mathbf{g}}_{-\eta}$ since we know $\mathbf{W}_i$ for all $i \in [n] \setminus \{\eta\}$. Note that we do not know $\mathbf{W}_\eta$ where there is a secret vector $\mathbf{v}$, but it is not needed here.

Simulating $\mathbf{h}'_j$. Sample $\bar{\mathbf{r}}_j \leftarrow \mathbb{Z}_p^k$ and implicitly define

$$\mathbf{r}'_j = \mathbf{Z}\bar{\mathbf{r}}_j \quad \text{for all } j \in [q].$$

We are ready to produce $\big[\mathbf{r}'_j\big]_2$ and $\big[\mathbf{W}_i^\top \mathbf{r}'_j\big]_2$ for $i \in [n] \setminus \{\eta\}$. Observe that

$$\mathbf{W}_\eta^\top \mathbf{r}'_j = \big(\bar{\mathbf{W}}_\eta + \mathbf{v}^\top {\mathbf{a}^\perp}^\top\big)^\top \mathbf{Z}\bar{\mathbf{r}}_j = \bar{\mathbf{W}}_\eta^\top \mathbf{Z}\bar{\mathbf{r}}_j + \mathbf{a}^\perp\,(\mathbf{v}\mathbf{Z})\,\bar{\mathbf{r}}_j.$$

The entry $\big[\mathbf{W}_\eta^\top \mathbf{r}'_j\big]_2$ can be simulated with $\bar{\mathbf{W}}_\eta$, $\mathbf{a}^\perp$, $\bar{\mathbf{r}}_j$ and $[\mathbf{Z}]_2, [\mathbf{v}\mathbf{Z}]_2$.

Simulating the challenge. For all $j \in [q]$, we produce the challenge as

$$\big([\boldsymbol{\tau}_j]_2, \big[\mathbf{W}_1^\top \boldsymbol{\tau}_j\big]_2, \ldots, \big[\bar{\mathbf{W}}_\eta^\top \boldsymbol{\tau}_j + \mathbf{a}^\perp \tau_j\big]_2, \ldots, \big[\mathbf{W}_n^\top \boldsymbol{\tau}_j\big]_2\big).$$

Here we implicitly set $\mathbf{r}_j = \boldsymbol{\tau}_j$. Observe that, when $\mathbf{t}_j \leftarrow \mathsf{Span}(\mathbf{M})$, we have $\tau_j = \mathbf{v}\boldsymbol{\tau}_j$, the challenge is identical to $\{\mathbf{h}_j\}$, i.e., $\gamma_j = 0$; when $\mathbf{t}_j \leftarrow \mathbb{Z}_p^{k+1}$, we have $\tau_j \leftarrow \mathbb{Z}_p$, the challenge is identical to $\{\mathbf{h}_j \cdot (1_{\mathbb{H}_0}; (h^*)^{\gamma_j \mathbf{e}_\eta})\}$ where $\gamma_j = \tau_j - \mathbf{v}\boldsymbol{\tau}_j$ is uniformly distributed over $\mathbb{Z}_p$. This proves the lemma. □

5 Towards Tight Security in MIMC Setting

5.1 A Generalization of Extended Nested Dual System Group

Applying Gong *et al.*'s idea of extending NDSG [14], a variant of Hofheinz *et al.*'s method [18], to our generalization described in Section 4.1, we obtain a generalization of extended nested dual system group (ENDSG).

Algorithms. Our ENDSG consists of eight p.p.t. algorithms defined as follows:

- $\mathsf{SampP}(1^\lambda, n)$: Output $(\textsc{pp}, \textsc{sp})$ where:
  - $\textsc{pp}$ contains group description $(\mathbb{G}_0, \mathbb{G}, \mathbb{H}_0, \mathbb{H}, \mathbb{G}_T)$ and two admissible bilinear maps
$$e_0 : \mathbb{G}_0 \times \mathbb{H} \to \mathbb{G}_T \quad \text{and} \quad e : \mathbb{G} \times \mathbb{H}_0 \to \mathbb{G}_T,$$
an efficient linear map μ defined on $\mathbb{H}$, and public parameters for SampG;
  - $\textsc{sp}$ contains secret parameters for SampH, $\widehat{\mathsf{SampG}}$, $\widetilde{\mathsf{SampG}}$, $\widehat{\mathsf{SampH}}^*$, and $\widetilde{\mathsf{SampH}}^*$.
- SampGT: $\mathrm{Im}(\mu) \to \mathbb{G}_T$.
- $\mathsf{SampG}(\textsc{pp})$: Output $\mathbf{g} = (g_0;\ g_1,\ \ldots,\ g_n) \in \mathbb{G}_0 \times \mathbb{G}^n$.
- $\mathsf{SampH}(\textsc{pp}, \textsc{sp})$: Output $\mathbf{h} = (h_0;\ h_1,\ \ldots,\ h_n) \in \mathbb{H}_0 \times \mathbb{H}^n$.
- $\widehat{\mathsf{SampG}}(\textsc{pp}, \textsc{sp})$: Output $\widehat{\mathbf{g}} = (\widehat{g}_0;\ \widehat{g}_1,\ \ldots,\ \widehat{g}_n) \in \mathbb{G}_0 \times \mathbb{G}^n$.
- $\widetilde{\mathsf{SampG}}(\textsc{pp}, \textsc{sp})$: Output $\widetilde{\mathbf{g}} = (\widetilde{g}_0;\ \widetilde{g}_1,\ \ldots,\ \widetilde{g}_n) \in \mathbb{G}_0 \times \mathbb{G}^n$.
- $\widehat{\mathsf{SampH}}^*(\textsc{pp}, \textsc{sp})$: Output $\widehat{h}^* \in \mathbb{H}$.
- $\widetilde{\mathsf{SampH}}^*(\textsc{pp}, \textsc{sp})$: Output $\widetilde{h}^* \in \mathbb{H}$.

We employ SampG_0 (resp., $\widehat{\mathsf{SampG}}_0$, $\widetilde{\mathsf{SampG}}_0$) to indicate the first element $g_0 \in \mathbb{G}_0$ (resp., $\widehat{g}_0 \in \mathbb{G}_0$, $\widetilde{g}_0 \in \mathbb{G}_0$) in the output of SampG (resp., $\widehat{\mathsf{SampG}}$, $\widetilde{\mathsf{SampG}}$).

Correctness and Security. The correctness requirement is exactly the same as our generalized NDSG including *projective* and *associative* (c.f. Section 4.1). For all $\lambda, n \in \mathbb{Z}^+$ and $(\textsc{pp}, \textsc{sp}) \leftarrow \mathsf{SampP}(1^\lambda, n)$, the security requirement involves:

(orthogonality) For all $\widehat{h}^* \in [\widehat{\mathsf{SampH}}^*(\textsc{pp}, \textsc{sp})]$ and all $\widetilde{h}^* \in [\widetilde{\mathsf{SampH}}^*(\textsc{pp}, \textsc{sp})]$, (1) $\mu(\widehat{h}^*) = \mu(\widetilde{h}^*) = 1$; (2) $e_0(\widehat{g}_0, \widetilde{h}^*) = 1$ for all $\widehat{g}_0 \in [\widehat{\mathsf{SampG}}_0(\textsc{pp}, \textsc{sp})]$; (3) $e_0(\widetilde{g}_0, \widehat{h}^*) = 1$ for all $\widetilde{g}_0 \in [\widetilde{\mathsf{SampG}}_0(\textsc{pp}, \textsc{sp})]$.

($\mathbb{H}$-subgroup) The output of $\mathsf{SampH}(\textsc{pp}, \textsc{sp})$ is uniformly distributed over some subgroup of $\mathbb{H}_0 \times \mathbb{H}^n$, while those of $\widehat{\mathsf{SampH}}^*(\textsc{pp}, \textsc{sp})$ and $\widetilde{\mathsf{SampH}}^*(\textsc{pp}, \textsc{sp})$ are uniformly distributed over some subgroup of $\mathbb{H}$, respectively.

(left subgroup indistinguishability 1) For any p.p.t. adversary $\mathcal{A}$, the following advantage function is negligible in λ.

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{LS1}}(\lambda, q, q') := \left|\Pr[\mathcal{A}(D, T_0) = 1] - \Pr[\mathcal{A}(D, T_1) = 1]\right|,$$

where $D = \big(\textsc{pp}, \{\mathbf{h}_j\}_{j\in[q']}\big)$,

$$T_0 = \{\mathbf{g}_j\}_{j\in[q]}, \quad T_1 = \big\{\mathbf{g}_j \cdot \boxed{\widehat{\mathbf{g}}_j \cdot \widetilde{\mathbf{g}}_j}\big\}_{j\in[q]}$$

and $\mathbf{g}_j \leftarrow \mathsf{SampG}(\textsc{pp})$, $\widehat{\mathbf{g}}_j \leftarrow \widehat{\mathsf{SampG}}(\textsc{pp}, \textsc{sp})$, $\widetilde{\mathbf{g}}_j \leftarrow \widetilde{\mathsf{SampG}}(\textsc{pp}, \textsc{sp})$, $\mathbf{h}_j \leftarrow \mathsf{SampH}(\textsc{pp}, \textsc{sp})$.

(left subgroup indistinguishability 2) For any p.p.t. adversary $\mathcal{A}$, the following advantage function is negligible in λ.

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{LS2}}(\lambda, q, q') = \left|\Pr[\mathcal{A}(D, T_0) = 1] - \Pr[\mathcal{A}(D, T_1) = 1]\right|,$$

where $D = \left(\textsc{pp}, \left\{\widehat{h}_j^* \cdot \widetilde{h}_j^*\right\}_{j\in[q+q']}, \left\{\mathbf{g}'_j \cdot \widehat{\mathbf{g}}'_j \cdot \widetilde{\mathbf{g}}'_j\right\}_{j\in[q]}, \left\{\mathbf{h}_j\right\}_{j\in[q']}\right)$,

$$T_0 = \left\{\mathbf{g}_j \cdot \widehat{\mathbf{g}}_j \cdot \boxed{\widetilde{\mathbf{g}}_j}\right\}_{j\in[q]}, \quad T_1 = \left\{\mathbf{g}_j \cdot \widehat{\mathbf{g}}_j\right\}_{j\in[q]},$$

and $\widehat{h}_j^* \leftarrow \widehat{\mathsf{SampH}}^*(\textsc{pp}, \textsc{sp})$, $\widetilde{h}_j^* \leftarrow \widetilde{\mathsf{SampH}}^*(\textsc{pp}, \textsc{sp})$, $\mathbf{g}_j, \mathbf{g}'_j \leftarrow \mathsf{SampG}(\textsc{pp})$, $\widehat{\mathbf{g}}_j, \widehat{\mathbf{g}}'_j \leftarrow \widehat{\mathsf{SampG}}(\textsc{pp}, \textsc{sp})$, $\widetilde{\mathbf{g}}_j, \widetilde{\mathbf{g}}'_j \leftarrow \widetilde{\mathsf{SampG}}(\textsc{pp}, \textsc{sp})$, $\mathbf{h}_j \leftarrow \mathsf{SampH}(\textsc{pp}, \textsc{sp})$.

(left subgroup indistinguishability 3) For any p.p.t. adversary $\mathcal{A}$, the following advantage function is negligible in λ.

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{LS3}}(\lambda, q, q') = \left|\Pr[\mathcal{A}(D, T_0) = 1] - \Pr[\mathcal{A}(D, T_1) = 1]\right|,$$

where $D = \left(\textsc{pp}, \left\{\widehat{h}_j^* \cdot \widetilde{h}_j^*\right\}_{j\in[q+q']}, \left\{\mathbf{g}'_j \cdot \widehat{\mathbf{g}}'_j\right\}_{j\in[q]}, \left\{\mathbf{h}_j\right\}_{j\in[q']}\right)$,

$$T_0 = \left\{\mathbf{g}_j \cdot \boxed{\widehat{\mathbf{g}}_j} \cdot \widetilde{\mathbf{g}}_j\right\}_{j\in[q]}, \quad T_1 = \left\{\mathbf{g}_j \cdot \widetilde{\mathbf{g}}_j\right\}_{j\in[q]},$$

and $\widehat{h}_j^* \leftarrow \widehat{\mathsf{SampH}}^*(\textsc{pp}, \textsc{sp})$, $\widetilde{h}_j^* \leftarrow \widetilde{\mathsf{SampH}}^*(\textsc{pp}, \textsc{sp})$, $\mathbf{g}_j, \mathbf{g}'_j \leftarrow \mathsf{SampG}(\textsc{pp})$, $\widehat{\mathbf{g}}_j, \widehat{\mathbf{g}}'_j \leftarrow \widehat{\mathsf{SampG}}(\textsc{pp}, \textsc{sp})$, $\widetilde{\mathbf{g}}_j \leftarrow \widetilde{\mathsf{SampG}}(\textsc{pp}, \textsc{sp})$, $\mathbf{h}_j \leftarrow \mathsf{SampH}(\textsc{pp}, \textsc{sp})$.

(nested-hiding indistinguishability) For all $\eta \in [\lfloor n/2 \rfloor]$ and any p.p.t. adversary $\mathcal{A}$, the following advantage function is negligible in λ.

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{NH}(\eta)}(\lambda, q, q') = \left|\Pr[\mathcal{A}(D, T_0) = 1] - \Pr[\mathcal{A}(D, T_1) = 1]\right|,$$

where $D = \left(\textsc{pp}, \left\{\widehat{h}_j^*, \widetilde{h}_j^*\right\}_{j\in[q+q']}, \left\{(\widehat{\mathbf{g}}_j)_{-(2\eta-1)}, (\widetilde{\mathbf{g}}_j)_{-2\eta}\right\}_{j\in[q]}, \left\{\mathbf{h}'_j\right\}_{j\in[q']}\right)$,

$$T_0 = \left\{\mathbf{h}_j\right\}_{j\in[q']}, \quad T_1 = \left\{\mathbf{h}_j \cdot \boxed{(1_{\mathbb{H}_0}; (\widehat{h}_j^{**})^{\mathbf{e}_{2\eta-1}}) \cdot (1_{\mathbb{H}_0}; (\widetilde{h}_j^{**})^{\mathbf{e}_{2\eta}})}\right\}_{j\in[q']}$$

and $\widehat{\mathbf{g}}_j \leftarrow \widehat{\mathsf{SampG}}(\textsc{pp}, \textsc{sp})$, $\widetilde{\mathbf{g}}_j \leftarrow \widetilde{\mathsf{SampG}}(\textsc{pp}, \textsc{sp})$, $\widehat{h}_j^*, \widehat{h}_j^{**} \leftarrow \widehat{\mathsf{SampH}}^*(\textsc{pp}, \textsc{sp})$, $\widetilde{h}_j^*, \widetilde{h}_j^{**} \leftarrow \widetilde{\mathsf{SampH}}^*(\textsc{pp}, \textsc{sp})$, $\mathbf{h}_j, \mathbf{h}'_j \leftarrow \mathsf{SampH}(\textsc{pp}, \textsc{sp})$. We may further define $\mathsf{Adv}_{\mathcal{A}}^{\mathrm{NH}}(\lambda, q, q') = \max_{\eta\in[\lfloor n/2 \rfloor]}\{\mathsf{Adv}_{\mathcal{A}}^{\mathrm{NH}(\eta)}(\lambda, q, q')\}$.

(non-degeneracy) For any p.p.t. adversary $\mathcal{A}$, the following advantage function is negligible in λ.

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{ND}}(\lambda, q, q', q'') = \left|\Pr[\mathcal{A}(D, T_0) = 1] - \Pr[\mathcal{A}(D, T_1) = 1]\right|,$$

where $D = \left(\textsc{pp}, \left\{\widehat{h}_j^* \cdot \widetilde{h}_j^*,\ \mathbf{h}_j\right\}_{j\in[q']}, \left\{\widehat{\mathbf{g}}_{j,j'} = (\widehat{g}_{0,j,j'}; \ldots)\right\}_{j\in[q], j'\in[q'']}\right)$,

$$T_0 = \left\{e_0(\widehat{g}_{0,j,j'}, \widehat{h}_j^{**})\right\}_{j\in[q], j'\in[q'']}, \; T_1 = \left\{e_0(\widehat{g}_{0,j,j'}, \widehat{h}_j^{**}) \cdot \boxed{R_{j,j'}}\right\}_{j\in[q], j'\in[q'']}$$

and $\widehat{\mathbf{g}}_{j,j'} \leftarrow \widehat{\mathsf{SampG}}(\textsc{pp}, \textsc{sp})$, $\widetilde{h}_j^* \leftarrow \widetilde{\mathsf{SampH}}^*(\textsc{pp}, \textsc{sp})$, $\widehat{h}_j^*, \widehat{h}_j^{**} \leftarrow \widehat{\mathsf{SampH}}^*(\textsc{pp}, \textsc{sp})$, $\mathbf{h}_j \leftarrow \mathsf{SampH}(\textsc{pp}, \textsc{sp})$, and $R_{j,j'} \leftarrow \mathbb{G}_T$.

($\mathbb{G}$-uniformity) For any p.p.t. adversary $\mathcal{A}$, the following advantage function is negligible in λ.

$$\mathsf{Adv}_{\mathcal{A}}^{\mathbb{G}\text{-uni}}(\lambda, q, q') = |\Pr[\mathcal{A}(D, T_0) = 1] - \Pr[\mathcal{A}(D, T_1) = 1]|\,,$$

where $D = \big(\textsc{pp}, \big\{\mathbf{h}_j \cdot (1_{\mathbb{H}_0};\ \widehat{h}^*_{1,j}, \ldots, \widehat{h}^*_{n,j}),\ \widehat{h}^*_j,\ \widetilde{h}^*_j\big\}_{j\in[q']}\big)$,

$$T_0 = \{\mathbf{g}_j \cdot \widehat{\mathbf{g}}_j\}_{j\in[q]}, \quad T_1 = \big\{\mathbf{g}_j \cdot \widehat{\mathbf{g}}_j \cdot \boxed{(1_{\mathbb{G}_0}; (g'_j)^{\mathbf{1}_n})}\big\}_{j\in[q]}$$

and $\mathbf{h}_j \leftarrow \mathsf{SampH}(\textsc{pp}, \textsc{sp})$, $\mathbf{g}_j \leftarrow \mathsf{SampG}(\textsc{pp})$, $\widehat{\mathbf{g}}_j \leftarrow \widehat{\mathsf{SampG}}(\textsc{pp}, \textsc{sp})$, $\widetilde{h}^*_j \leftarrow \widetilde{\mathsf{SampH}}^*(\textsc{pp}, \textsc{sp})$, $\widehat{h}^*_j, \widehat{h}^*_{1,j}, \ldots, \widehat{h}^*_{n,j} \leftarrow \widehat{\mathsf{SampH}}^*(\textsc{pp}, \textsc{sp})$, $g'_j \leftarrow \mathbb{G}$.

The generic IBE in the multi-instance setting is similar to the IBE scheme in Section 4.1 except that we take $(\textsc{pp}, \textsc{sp}) \leftarrow \mathsf{SampP}(1^\lambda, 2n)$ as the global parameter $\textsc{gp}$ and master secret $\textsc{msk}_0 \in \mathbb{H}$ will be picked for each instance (in algorithm Setup).

5.2 An Instantiation in the Prime-order Group

The generalized ENDSG described above can be implemented by extending the construction in Section 4.2. In particular, we follow the extension technique by Gong *et al.* [14] and Gay *et al.* [12] (c.f. Section 3.3).

- $\mathsf{SampP}(1^\lambda, n)$: Run $\mathcal{G} = (G_1, G_2, G_T, p, e, g_1, g_2) \leftarrow \mathsf{GrpGen}(1^\lambda)$. Define

$$\mathbb{G}_0 = G_1^{3k}, \quad \mathbb{G} = G_1^k, \quad \mathbb{H}_0 = G_2^k, \quad \mathbb{H} = G_2^{3k}$$

and bilinear map e_0 and e are natural extension of e (given in $\mathcal{G}$) to $3k$-dim and k-dim, respectively. Sample $\mathbf{A}, \widehat{\mathbf{A}}, \widetilde{\mathbf{A}} \leftarrow \mathcal{U}_{3k,k}$ and randomly pick $\widehat{\mathbf{A}}^*, \widetilde{\mathbf{A}}^* \in \mathbb{Z}_p^{3k\times k}$ as respective bases of $\mathsf{Ker}\big((\mathbf{A}|\widetilde{\mathbf{A}})^\top\big)$ and $\mathsf{Ker}\big((\mathbf{A}|\widehat{\mathbf{A}})^\top\big)$. For each $\mathbf{k} \in \mathbb{Z}_p^{3k}$, define $\mu : G_2^{3k} \to G_T^k$ by $\mu([\mathbf{k}]_2) = e([\mathbf{A}]_1, [\mathbf{k}]_2) = [\mathbf{A}^\top\mathbf{k}]_T$. Sample $\mathbf{W}_i \leftarrow \mathbb{Z}_p^{k\times 3k}$ for all $i \in [n]$ and output

$$\textsc{pp} = \big([\mathbf{A}]_1, [\mathbf{W}_1\mathbf{A}]_1, \ldots, [\mathbf{W}_n\mathbf{A}]_1\big), \quad \textsc{sp} = \big(\widehat{\mathbf{A}}, \widetilde{\mathbf{A}}, \widehat{\mathbf{A}}^*, \widetilde{\mathbf{A}}^*, \mathbf{W}_1, \ldots, \mathbf{W}_n\big).$$

- $\mathsf{SampGT}([\mathbf{p}]_T)$: Sample $\mathbf{s} \leftarrow \mathbb{Z}_p^k$ and output $[\mathbf{s}^\top\mathbf{p}]_T$ for $\mathbf{p} \in \mathbb{Z}_p^k$.
- $\mathsf{SampG}(\textsc{pp})$: Sample $\mathbf{s} \leftarrow \mathbb{Z}_p^k$ and output

$$\big([\mathbf{A}\mathbf{s}]_1;\ [\mathbf{W}_1\mathbf{A}\mathbf{s}]_1,\ \ldots,\ [\mathbf{W}_n\mathbf{A}\mathbf{s}]_1\big) \in G_1^{3k} \times (G_1^k)^n.$$

- $\mathsf{SampH}(\textsc{pp}, \textsc{sp})$: Sample $\mathbf{r} \leftarrow \mathbb{Z}_p^k$ and output

$$\big([\mathbf{r}]_2;\ [\mathbf{W}_1^\top\mathbf{r}]_2,\ \ldots,\ [\mathbf{W}_n^\top\mathbf{r}]_2\big) \in G_2^k \times (G_2^{3k})^n.$$

- $\widehat{\mathsf{SampG}}(\textsc{pp}, \textsc{sp})$: Sample $\widehat{\mathbf{s}} \leftarrow \mathbb{Z}_p^k$ and output

$$\big([\widehat{\mathbf{A}}\widehat{\mathbf{s}}]_1;\ [\mathbf{W}_1\widehat{\mathbf{A}}\widehat{\mathbf{s}}]_1,\ \ldots,\ [\mathbf{W}_n\widehat{\mathbf{A}}\widehat{\mathbf{s}}]_1\big) \in G_1^{3k} \times (G_1^k)^n.$$

- $\widetilde{\mathsf{SampG}}(\textsc{pp}, \textsc{sp})$: Sample $\widetilde{\mathbf{s}} \leftarrow \mathbb{Z}_p^k$ and output

$$\big([\widetilde{\mathbf{A}}\widetilde{\mathbf{s}}]_1;\ [\mathbf{W}_1\widetilde{\mathbf{A}}\widetilde{\mathbf{s}}]_1,\ \ldots,\ [\mathbf{W}_n\widetilde{\mathbf{A}}\widetilde{\mathbf{s}}]_1\big) \in G_1^{3k} \times (G_1^k)^n.$$

- $\widehat{\mathsf{SampH}}^*(\textsc{pp}, \textsc{sp})$: Sample $\widehat{\mathbf{r}} \in \mathbb{Z}_p^k$ and output $\big[\widehat{\mathbf{A}}^*\widehat{\mathbf{r}}\big]_2 \in G_2^{3k}$.
- $\widetilde{\mathsf{SampH}}^*(\textsc{pp}, \textsc{sp})$: Sample $\widetilde{\mathbf{r}} \in \mathbb{Z}_p^k$ and output $\big[\widetilde{\mathbf{A}}^*\widetilde{\mathbf{r}}\big]_2 \in G_2^{3k}$.

For the lack of space, we only show that our instantiation satisfies *Left Subgroup Indistinguishability 2* and *3*, *Nested-hiding Indistinguishability* and $\mathbb{G}$-*uniformity* in the next several subsections.

5.3 Left Subgroup Indistinguishability 2 & 3

We rewrite the advantage function $\mathsf{Adv}_{\mathcal{A}}^{\mathrm{LS2}}(k, q, q')$ using

$$\begin{aligned}
\textsc{pp} &= \big([\mathbf{A}]_1,\ [\mathbf{W}_1\mathbf{A}]_1,\ \ldots,\ [\mathbf{W}_n\mathbf{A}]_1\big)\,;\\
\widehat{h}_j^* \cdot \widetilde{h}_j^* &= \big[\widehat{\mathbf{A}}^*\widehat{\mathbf{r}}_j + \widetilde{\mathbf{A}}^*\widetilde{\mathbf{r}}_j\big]_2,\ \widehat{\mathbf{r}}_j, \widetilde{\mathbf{r}}_j \leftarrow \mathbb{Z}_p^k;\\
\mathbf{g}_j' \cdot \widehat{\mathbf{g}}_j' \cdot \widetilde{\mathbf{g}}_j' &= \big([\mathbf{s}_j']_1;\ [\mathbf{W}_1\mathbf{s}_j']_1,\ \ldots,\ [\mathbf{W}_n\mathbf{s}_j']_1\big),\ \mathbf{s}_j' \leftarrow \mathbb{Z}_p^{3k};\\
\mathbf{h}_j &= \big([\mathbf{r}_j]_2;\ [\mathbf{W}_1^\top\mathbf{r}_j]_2,\ \ldots,\ [\mathbf{W}_n^\top\mathbf{r}_j]_2\big),\ \mathbf{r}_j \leftarrow \mathbb{Z}_p^k;\\
\mathbf{g}_j \cdot \widehat{\mathbf{g}}_j &= \big(\big[\mathbf{A}\mathbf{s}_j + \widehat{\mathbf{A}}\widehat{\mathbf{s}}_j\big]_1;\ \big[\mathbf{W}_1(\mathbf{A}\mathbf{s}_j + \widehat{\mathbf{A}}\widehat{\mathbf{s}}_j)\big]_1,\ \ldots,\ \big[\mathbf{W}_n(\mathbf{A}\mathbf{s}_j + \widehat{\mathbf{A}}\widehat{\mathbf{s}}_j)\big]_1\big),\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\mathbf{s}_j, \widehat{\mathbf{s}}_j \leftarrow \mathbb{Z}_p^k;\\
\mathbf{g}_j \cdot \widehat{\mathbf{g}}_j \cdot \widetilde{\mathbf{g}}_j &= \big([\mathbf{s}_j]_1;\ [\mathbf{W}_1\mathbf{s}_j]_1,\ \ldots,\ [\mathbf{W}_n\mathbf{s}_j]_1\big),\ \mathbf{s}_j \leftarrow \mathbb{Z}_p^{3k}.
\end{aligned}$$

Note that the distribution here is identical to the original one except that $\mathbf{A}$, $\widehat{\mathbf{A}}$, $\widetilde{\mathbf{A}}$ fail to span the entire space $\mathbb{Z}_p^{3k}$ whose probability is bounded by $2k/p$ (c.f. Lemma 3). We prove the following lemma.

Lemma 7. *For any p.p.t. adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$ such that*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{LS2}}(\lambda, q, q') \leqslant \mathsf{Adv}_{\mathcal{B},q}^{\mathcal{U}_{3k,k}}(\lambda) + 2^{-\Omega(\lambda)}$$

where $\mathsf{T}(\mathcal{B}) \approx \mathsf{T}(\mathcal{A}) + k^2 \cdot (q+q') \cdot \mathsf{poly}(\lambda, n)$ *and* $\mathsf{poly}(\lambda, n)$ *is independent of* $\mathsf{T}(\mathcal{A})$.

Proof. Given $[\widehat{\mathbf{A}}]_1 \in G_1^{3k \times k}$ and $[\mathbf{T}]_1 = [\mathbf{t}_1|\cdots|\mathbf{t}_q]_1 \in G_1^{3k \times q}$, $\mathcal{B}$ works as follows:

Simulating pp. Sample $\mathbf{A} \leftarrow \mathcal{U}_{3k,k}$ and $\mathbf{W}_i \leftarrow \mathbb{Z}_p^{k \times 3k}$ for all $i \in [n]$. We can then simulate $\textsc{pp}$ directly.

Simulating $\widehat{h}_j^* \cdot \widetilde{h}_j^*$. Calculate $\mathbf{A}^\perp \in \mathbb{Z}_p^{3k \times 2k}$ from $\mathbf{A} \in \mathbb{Z}_p^{3k \times k}$ and one may simulate $\widehat{h}_j^* \cdot \widetilde{h}_j^*$ by sampling $\widehat{h}_j^* \cdot \widetilde{h}_j^* \leftarrow \mathsf{Span}([\mathbf{A}^\perp]_2)$ by Lemma 3.

Simulating $\mathbf{g}_j' \cdot \widehat{\mathbf{g}}_j' \cdot \widetilde{\mathbf{g}}_j'$ and $\mathbf{h}_j$. We can simply simulate each $\mathbf{g}_j' \cdot \widehat{\mathbf{g}}_j' \cdot \widetilde{\mathbf{g}}_j'$ (resp. $\mathbf{h}_j$) using $\mathbf{W}_i$ for all $i \in [n]$ and a freshly chosen $\mathbf{s}_j' \leftarrow \mathbb{Z}_p^{3k}$ for all $j \in [q]$ (resp. $\mathbf{r}_j \in \mathbb{Z}_p^k$ for all $j \in [q']$).

Simulating the Challenge. Sample $\bar{\mathbf{s}}_j \leftarrow \mathbb{Z}_p^k$ for all $j \in [q]$. We simulate the challenge as

$$\big([\mathbf{A}\bar{\mathbf{s}}_j + \mathbf{t}_j]_1; [\mathbf{W}_1(\mathbf{A}\bar{\mathbf{s}}_j + \mathbf{t}_j)]_1, \ldots, [\mathbf{W}_n(\mathbf{A}\bar{\mathbf{s}}_j + \mathbf{t}_j)]_1\big) \quad \text{for all } j \in [q].$$

Observe that: when $\mathbf{t}_j \leftarrow \mathsf{Span}(\widehat{\mathbf{A}})$ for all $j \in [q]$, the challenge equals $\{\mathbf{g}_j \cdot \widehat{\mathbf{g}}_j\}$; when $\mathbf{t}_j \leftarrow \mathbb{Z}_p^{3k}$ for all $j \in [q]$, the challenge is identical to $\{\mathbf{g}_j \cdot \widehat{\mathbf{g}}_j \cdot \widetilde{\mathbf{g}}_j\}$ (we described above). This proves the lemma. □

We can prove a similar lemma for $\mathsf{Adv}_{\mathcal{A}}^{\mathrm{LS3}}(k, q, q')$. The proof is almost the same as above with the exception that $\mathcal{B}$ controls $\mathbf{A}$ and $\widehat{\mathbf{A}}$ this time, and embeds q-fold $\mathcal{U}_{3k,k}$-MDDH instance through $\widetilde{\mathbf{A}}$. More concretely, one may simulate PP, $\{\widehat{h}_j^* \cdot \widetilde{h}_j^*\}$, $\{\mathbf{h}_j\}$ and the challenge with $\mathbf{A}$ and $\widetilde{\mathbf{A}}$ as before, while the simulation of $\{\mathbf{g}'_j \cdot \widehat{\mathbf{g}}'_j\}$ needs the help of $\widehat{\mathbf{A}}$.

5.4 Nested-hiding Indistinguishability

For all $\eta \in [\lfloor n/2 \rfloor]$, we rewrite the advantage function $\mathsf{Adv}_{\mathcal{A}}^{\mathrm{NH}(\eta)}(\lambda, q, q')$ using

$$\begin{aligned}
\mathrm{PP} &= \big([\mathbf{A}]_1,\ [\mathbf{W}_1\mathbf{A}]_1,\ \ldots,\ [\mathbf{W}_n\mathbf{A}]_1\big);\\
\widehat{h}_j^* &= \big[\widehat{\mathbf{A}}^*\widehat{\mathbf{r}}'_j\big]_2,\ \widehat{\mathbf{r}}'_j \leftarrow \mathbb{Z}_p^k; \qquad \widetilde{h}_j^* = \big[\widetilde{\mathbf{A}}^*\widetilde{\mathbf{r}}'_j\big]_2,\ \widetilde{\mathbf{r}}'_j \leftarrow \mathbb{Z}_p^k;\\
\widehat{\mathbf{g}}_j &= \big([\widehat{\mathbf{A}}\widehat{\mathbf{s}}_j]_1;\ [\mathbf{W}_1\widehat{\mathbf{A}}\widehat{\mathbf{s}}_j]_1,\ \ldots,\ [\mathbf{W}_n\widehat{\mathbf{A}}\widehat{\mathbf{s}}_j]_1\big),\ \widehat{\mathbf{s}}_j \leftarrow \mathbb{Z}_p^k;\\
\widetilde{\mathbf{g}}_j &= \big([\widetilde{\mathbf{A}}\widetilde{\mathbf{s}}_j]_1;\ [\mathbf{W}_1\widetilde{\mathbf{A}}\widetilde{\mathbf{s}}_j]_1,\ \ldots,\ [\mathbf{W}_n\widetilde{\mathbf{A}}\widetilde{\mathbf{s}}_j]_1\big),\ \widetilde{\mathbf{s}}_j \leftarrow \mathbb{Z}_p^k;\\
\mathbf{h}'_j &= \big([\mathbf{r}'_j]_2;\ [\mathbf{W}_1^\top\mathbf{r}'_j]_2,\ \ldots,\ [\mathbf{W}_n^\top\mathbf{r}'_j]_2\big),\ \mathbf{r}'_j \leftarrow \mathbb{Z}_p^k
\end{aligned}$$

and the challenge term $\mathbf{h}_j \cdot (1_{\mathbb{H}_0}; (\widehat{h}_j^{**})^{\mathbf{e}_{2\eta-1}}) \cdot (1_{\mathbb{H}_0}; (\widetilde{h}_j^{**})^{\mathbf{e}_{2\eta}})$ equals

$$\big([\mathbf{r}_j]_2;\ \big[\mathbf{W}_1^\top\mathbf{r}_j\big]_2,\ \ldots,\ \big[\mathbf{W}_{2\eta-1}^\top\mathbf{r}_j + \widehat{\mathbf{A}}^*\widehat{\mathbf{r}}_j\big]_2,\ \big[\mathbf{W}_{2\eta}^\top\mathbf{r}_j + \widetilde{\mathbf{A}}^*\widetilde{\mathbf{r}}_j\big]_2,\ \ldots,\ \big[\mathbf{W}_n^\top\mathbf{r}_j\big]_2\big)$$

where $\mathbf{r}_j \leftarrow \mathbb{Z}_p^k$, either $\widehat{\mathbf{r}}_j, \widetilde{\mathbf{r}}_j \leftarrow \mathbb{Z}_p^k$ or $\widehat{\mathbf{r}}_j = \widetilde{\mathbf{r}}_j = \mathbf{0}_k$. We prove the lemma below.

Lemma 8. *For any p.p.t. adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$ such that*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{NH}(\eta)}(\lambda, q, q') \leqslant \mathsf{Adv}_{\mathcal{B},q'}^{\mathcal{U}_{3k,k}}(\lambda)$$

where $\mathsf{T}(\mathcal{B}) \approx \mathsf{T}(\mathcal{A}) + k^2 \cdot (q+q') \cdot \mathsf{poly}(\lambda, n)$ *and* $\mathsf{poly}(\lambda, n)$ *is independent of* $\mathsf{T}(\mathcal{A})$.

Before we prove the lemma, we describe and prove an extension of Lemma 5.

Lemma 9. *Given $Q \in \mathbb{N}$, group G of prime order p, $[\mathbf{M}] \in G^{3k\times k}$ and $[\mathbf{T}] = [\mathbf{t}_1|\cdots|\mathbf{t}_Q] \in G^{3k\times Q}$ where either $\mathbf{t}_i \leftarrow \mathsf{Span}(\mathbf{M})$ or $\mathbf{t}_i \leftarrow \mathbb{Z}_p^{3k}$, one can efficiently compute*

$$[\mathbf{Z}], \quad [\mathbf{V}_0\mathbf{Z}], \quad [\mathbf{V}_1\mathbf{Z}], \quad \big\{[\boldsymbol{\tau}_j], [\boldsymbol{\tau}_{0,j}], [\boldsymbol{\tau}_{1,j}]\big\}_{j\in[Q]}$$

where $\mathbf{Z} \in \mathbb{Z}_p^{k\times k}$ is full-rank, $\mathbf{V}_0, \mathbf{V}_1 \in \mathbb{Z}_p^{k\times k}$ are secret matrices, $\boldsymbol{\tau}_j \leftarrow \mathbb{Z}_p^k$ and either $\boldsymbol{\tau}_{0,j} = \mathbf{V}_0\boldsymbol{\tau}_j$, $\boldsymbol{\tau}_{1,j} = \mathbf{V}_1\boldsymbol{\tau}_j$ (when $\mathbf{t}_j \leftarrow \mathsf{Span}(\mathbf{M})$) or $\boldsymbol{\tau}_{0,j}, \boldsymbol{\tau}_{1,j} \leftarrow \mathbb{Z}_p^k$ (when $\mathbf{t}_j \leftarrow \mathbb{Z}_p^{3k}$).

Proof. Given Q, G, $[\mathbf{M}]$, $[\mathbf{T}] = [\mathbf{t}_1|\cdots|\mathbf{t}_Q]$, the algorithm works as follows:

Programming $[\mathbf{Z}], [\mathbf{V}_0\mathbf{Z}], [\mathbf{V}_1\mathbf{Z}]$. Define $\mathbf{Z} = \overline{\mathbf{M}}$. Randomly pick $\mathbf{M}_0, \mathbf{M}_1 \leftarrow \mathbb{Z}_p^{k\times 3k}$ and implicitly define $\mathbf{V}_0, \mathbf{V}_1 \in \mathbb{Z}_p^{k\times k}$ such that

$$\mathbf{V}_0\mathbf{Z} = \mathbf{V}_0\overline{\mathbf{M}} = \mathbf{M}_0\mathbf{M} \quad \text{and} \quad \mathbf{V}_1\mathbf{Z} = \mathbf{V}_1\overline{\mathbf{M}} = \mathbf{M}_1\mathbf{M}.$$

One can generate $[\mathbf{Z}]$ along with $[\mathbf{V}_0\mathbf{Z}], [\mathbf{V}_1\mathbf{Z}]$ using $[\mathbf{M}]$ and $\mathbf{M}_0, \mathbf{M}_1$.

Generating Q tuples. For all $j \in [Q]$, we compute

$$[\boldsymbol{\tau}_j] = [\overline{\mathbf{t}}_j], \quad [\boldsymbol{\tau}_{0,j}] = [\mathbf{M}_0\mathbf{t}_j], \quad [\boldsymbol{\tau}_{1,j}] = [\mathbf{M}_1\mathbf{t}_j].$$

Here $\overline{\mathbf{t}}_j$ indicates the first k entries of $\mathbf{t}_j$.

Observe that: if $\mathbf{t}_j = \mathbf{M}\mathbf{u}_j$ for some $\mathbf{u}_j \leftarrow \mathbb{Z}_p^k$, we have that $\boldsymbol{\tau}_j = \overline{\mathbf{M}}\mathbf{u}_j$ and

$$\boldsymbol{\tau}_{0,j} = \mathbf{M}_0\mathbf{M}\mathbf{u}_j = \mathbf{V}_0\overline{\mathbf{M}}\mathbf{u}_j = \mathbf{V}_0\boldsymbol{\tau}_j, \qquad \boldsymbol{\tau}_{1,j} = \mathbf{M}_1\mathbf{M}\mathbf{u}_j = \mathbf{V}_1\overline{\mathbf{M}}\mathbf{u}_j = \mathbf{V}_1\boldsymbol{\tau}_j;$$

if $\mathbf{t}_j \leftarrow \mathbb{Z}_p^{3k}$, we can see that

$$\begin{pmatrix} \boldsymbol{\tau}_j \\ \boldsymbol{\tau}_{0,j} \\ \boldsymbol{\tau}_{1,j} \end{pmatrix} = \begin{pmatrix} \mathbf{I}_{k\times 3k} \\ \mathbf{M}_0 \\ \mathbf{M}_1 \end{pmatrix} \mathbf{t}_j$$

is uniformly distributed over $\mathbb{Z}_p^{3k}$ where the left-most k columns of $\mathbf{I}_{k\times 3k}$ form an identity matrix and remaining columns are zero vectors. □

We are ready to prove Lemma 8 by extending the strategy proving Lemma 6.

Proof. Given $[\mathbf{M}]_2 \in G_2^{3k\times k}$ and $[\mathbf{T}]_2 = [\mathbf{t}_1|\cdots|\mathbf{t}_{q'}]_2 \in G_2^{3k\times q'}$ where either $\mathbf{t}_j \leftarrow \mathsf{Span}(\mathbf{M})$ or $\mathbf{t}_j \leftarrow \mathbb{Z}_p^{3k}$, $\mathcal{B}$ proceeds as follows:

Generating q' tuples. We invoke the algorithm described in Lemma 9 on input $(q', G_2, [\mathbf{M}]_2, [\mathbf{T}]_2)$ and obtain

$$\big([\mathbf{Z}]_2, [\mathbf{V}_0\mathbf{Z}]_2, [\mathbf{V}_1\mathbf{Z}]_2, \{[\boldsymbol{\tau}_j]_2, [\boldsymbol{\tau}_{0,j}]_2, [\boldsymbol{\tau}_{1,j}]_2\}_{j\in[q']}\big).$$

Simulating pp. Sample $\mathbf{A}, \widehat{\mathbf{A}}, \widetilde{\mathbf{A}} \leftarrow \mathcal{U}_{3k,k}$ and randomly pick $\widehat{\mathbf{A}}^*$ and $\widetilde{\mathbf{A}}^*$, the respective bases of $\mathsf{Ker}\big((\mathbf{A}|\widetilde{\mathbf{A}})^\top\big)$ and $\mathsf{Ker}\big((\mathbf{A}|\widehat{\mathbf{A}})^\top\big)$. Select $\bar{\mathbf{W}}_{2\eta-1}, \bar{\mathbf{W}}_{2\eta} \leftarrow \mathbb{Z}_p^{k\times 3k}$ and define

$$\mathbf{W}_{2\eta-1} = \bar{\mathbf{W}}_{2\eta-1} + \mathbf{V}_1^\top \cdot (\widehat{\mathbf{A}}^*)^\top \quad \text{and} \quad \mathbf{W}_{2\eta} = \bar{\mathbf{W}}_{2\eta} + \mathbf{V}_0^\top \cdot (\widetilde{\mathbf{A}}^*)^\top.$$

Then we sample $\mathbf{W}_i \leftarrow \mathbb{Z}_p^{k\times 3k}$ for all $i \in [n] \setminus \{2\eta-1, 2\eta\}$. We can simulate PP using the following observation:

$$\mathbf{W}_{2\eta-1}\mathbf{A} = \big(\bar{\mathbf{W}}_{2\eta-1} + \mathbf{V}_1^\top \cdot (\widehat{\mathbf{A}}^*)^\top\big)\mathbf{A} = \bar{\mathbf{W}}_{2\eta-1}\mathbf{A},$$
$$\mathbf{W}_{2\eta}\mathbf{A} = \big(\bar{\mathbf{W}}_{2\eta} + \mathbf{V}_0^\top \cdot (\widetilde{\mathbf{A}}^*)^\top\big)\mathbf{A} = \bar{\mathbf{W}}_{2\eta}\mathbf{A}.$$

Simulating $\widehat{h}_j^*$ and $\widetilde{h}_j^*$. It is direct to simulate all $\widehat{h}_j^*$ and $\widetilde{h}_j^*$ using $\widehat{\mathbf{A}}^*$ and $\widetilde{\mathbf{A}}^*$.

Simulating $(\widehat{\mathbf{g}}_j)_{-(2\eta-1)}$ and $(\widetilde{\mathbf{g}}_j)_{-2\eta}$. We can simulate $(\widehat{\mathbf{g}}_j)_{-(2\eta-1)}$ following the fact that

$$\mathbf{W}_{2\eta}\widehat{\mathbf{A}} = \big(\bar{\mathbf{W}}_{2\eta} + \mathbf{V}_0^\top \cdot (\widetilde{\mathbf{A}}^*)^\top\big)\widehat{\mathbf{A}} = \bar{\mathbf{W}}_{2\eta}\widehat{\mathbf{A}}.$$

Similarly, we can also simulate $(\widetilde{\mathbf{g}}_j)_{-2\eta}$ because

$$\mathbf{W}_{2\eta-1}\widetilde{\mathbf{A}} = \big(\bar{\mathbf{W}}_{2\eta-1} + \mathbf{V}_1^\top \cdot (\widehat{\mathbf{A}}^*)^\top\big)\widetilde{\mathbf{A}} = \bar{\mathbf{W}}_{2\eta}\widetilde{\mathbf{A}}.$$

Although $\mathbf{W}_{2\eta-1}\widehat{\mathbf{A}}$ and $\mathbf{W}_{2\eta}\widetilde{\mathbf{A}}$ contain secret matrices and are unknown to $\mathcal{B}$ due to Lemma 3, they are not necessary in our simulation.

Simulating $\mathbf{h}'_j$. Sample $\bar{\mathbf{r}}_j \leftarrow \mathbb{Z}_p^k$ and implicitly define $\mathbf{r}'_j = \mathbf{Z}\bar{\mathbf{r}}_j$ for all $j \in [q']$. We can simply produce $\big[\mathbf{r}'_j\big]_2$ and $\big[\mathbf{W}_i^\top\mathbf{r}'_j\big]_2$ for $i \in [n] \setminus \{2\eta-1, 2\eta\}$ while the remaining two entries are simulated following the fact

$$\mathbf{W}_{2\eta-1}^\top\mathbf{r}'_j = \big(\bar{\mathbf{W}}_{2\eta-1} + \mathbf{V}_1^\top \cdot (\widehat{\mathbf{A}}^*)^\top\big)^\top\mathbf{Z}\bar{\mathbf{r}}_j = \bar{\mathbf{W}}_{2\eta-1}^\top\mathbf{Z}\bar{\mathbf{r}}_j + \widehat{\mathbf{A}}^* \cdot (\mathbf{V}_1\mathbf{Z}) \cdot \bar{\mathbf{r}}_j,$$
$$\mathbf{W}_{2\eta}^\top\mathbf{r}'_j = \big(\bar{\mathbf{W}}_{2\eta} + \mathbf{V}_0^\top \cdot (\widetilde{\mathbf{A}}^*)^\top\big)^\top\mathbf{Z}\bar{\mathbf{r}}_j = \bar{\mathbf{W}}_{2\eta}^\top\mathbf{Z}\bar{\mathbf{r}}_j + \widetilde{\mathbf{A}}^* \cdot (\mathbf{V}_0\mathbf{Z}) \cdot \bar{\mathbf{r}}_j,$$

because $[\mathbf{Z}]_2$, $[\mathbf{V}_0\mathbf{Z}]_2$ and $[\mathbf{V}_1\mathbf{Z}]_2$ are known to $\mathcal{B}$.

Simulating the challenge. For all $j \in [q']$, we compute the challenge as

$$\big([\boldsymbol{\tau}_j]_2, [\mathbf{W}_1^\top\boldsymbol{\tau}_j]_2, \ldots, \big[\bar{\mathbf{W}}_{2\eta-1}^\top\boldsymbol{\tau}_j + \widehat{\mathbf{A}}^*\boldsymbol{\tau}_{1,j}\big]_2, \big[\bar{\mathbf{W}}_{2\eta}^\top\boldsymbol{\tau}_j + \widetilde{\mathbf{A}}^*\boldsymbol{\tau}_{0,j}\big]_2, \ldots, [\mathbf{W}_n^\top\boldsymbol{\tau}_j]_2\big).$$

Observe that, when $\mathbf{t}_j \leftarrow \mathsf{Span}(\mathbf{M})$, we have that $\boldsymbol{\tau}_{0,j} = \mathbf{V}_0\boldsymbol{\tau}_j$ and $\boldsymbol{\tau}_{1,j} = \mathbf{V}_1\boldsymbol{\tau}_j$, the challenge is identical to $\{\mathbf{h}_j\}$, i.e., $\widehat{\mathbf{r}}_j = \widetilde{\mathbf{r}}_j = \mathbf{0}_k$; when $\mathbf{t}_j \leftarrow \mathbb{Z}_p^{3k}$, we have $\boldsymbol{\tau}_{0,j}, \boldsymbol{\tau}_{1,j} \leftarrow \mathbb{Z}_p^k$, the challenge is identical to $\{\mathbf{h}_j \cdot (1_{\mathbb{H}_0}; (\widehat{h}_j^{**})^{\mathbf{e}_{2\eta-1}}) \cdot (1_{\mathbb{H}_0}; (\widetilde{h}_j^{**})^{\mathbf{e}_{2\eta}})\}$ where $\widehat{\mathbf{r}}_j = \boldsymbol{\tau}_{1,j} - \mathbf{V}_1\boldsymbol{\tau}_j$ and $\widetilde{\mathbf{r}}_j = \boldsymbol{\tau}_{0,j} - \mathbf{V}_0\boldsymbol{\tau}_j$ are uniformly distributed over $\mathbb{Z}_p^k$. This proves the lemma. □

5.5 $\mathbb{G}$-uniformity

We rewrite the advantage function $\mathsf{Adv}_{\mathcal{A}}^{\mathbb{G}\text{-uni}}(\lambda, q, q')$ using

$$\text{PP} = \big([\mathbf{A}]_1,\ [\mathbf{W}_1\mathbf{A}]_1,\ \ldots,\ [\mathbf{W}_n\mathbf{A}]_1\big);\quad \widehat{h}_j^* = \big[\widehat{\mathbf{A}}^*\widehat{\mathbf{r}}_j\big]_2;\quad \widetilde{h}_j^* = \big[\widetilde{\mathbf{A}}^*\widetilde{\mathbf{r}}_j\big]_2$$

where $\widehat{\mathbf{r}}_j, \widetilde{\mathbf{r}}_j \leftarrow \mathbb{Z}_p^k$ and $\mathbf{h}_j \cdot (1_{\mathbb{H}_0};\ \widehat{h}_{1,j}^*, \ldots, \widehat{h}_{n,j}^*)$ equals

$$\big([\mathbf{r}_j]_2;\ \big[\mathbf{W}_1^\top\mathbf{r}_j + \widehat{\mathbf{A}}^*\widehat{\mathbf{r}}_{1,j}\big]_2,\ \ldots,\ \big[\mathbf{W}_n^\top\mathbf{r}_j + \widehat{\mathbf{A}}^*\widehat{\mathbf{r}}_{n,j}\big]_2\big),\ \mathbf{r}_j, \widehat{\mathbf{r}}_{1,j}, \ldots, \widehat{\mathbf{r}}_{n,j} \leftarrow \mathbb{Z}_p^k;$$

and the challenge term $\mathbf{g}_j \cdot \widehat{\mathbf{g}}_j \cdot (1_{\mathbb{G}_0}; (g'_j)^{\mathbf{1}_n})$ equals

$$\big(\big[\mathbf{A}\mathbf{s}_j + \widehat{\mathbf{A}}\widehat{\mathbf{s}}_j\big]_1; \big[\mathbf{W}_1(\mathbf{A}\mathbf{s}_j + \widehat{\mathbf{A}}\widehat{\mathbf{s}}_j) + \mathbf{s}'_j\big]_1, \ldots, \big[\mathbf{W}_n(\mathbf{A}\mathbf{s}_j + \widehat{\mathbf{A}}\widehat{\mathbf{s}}_j) + \mathbf{s}'_j\big]_1\big)$$

where $\mathbf{s}_j, \widehat{\mathbf{s}}_j \leftarrow \mathbb{Z}_p^k$, either $\mathbf{s}'_j \leftarrow \mathbb{Z}_p^k$ or $\mathbf{s}'_j = \mathbf{0}_k$. We prove the following lemma using essentially the same method as in [3].

Lemma 10. *For any p.p.t. adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$ such that*

$$\mathsf{Adv}^{\mathbb{G}\text{-uni}}_{\mathcal{A}}(\lambda, q, q') \leqslant \mathsf{Adv}^{\mathcal{U}_{2k,k}}_{\mathcal{B},q}(\lambda)$$

where $\mathsf{T}(\mathcal{B}) \approx \mathsf{T}(\mathcal{A}) + k^2 \cdot (q+q') \cdot \mathsf{poly}(\lambda, n)$ *and* $\mathsf{poly}(\lambda, n)$ *is independent of* $\mathsf{T}(\mathcal{A})$.

We describe a simple extension of Lemma 5 without proof which is basically identical to *Generalized Many-Tuple Lemma* in [14].

Lemma 11. *Given $Q \in \mathbb{N}$, group G of prime order p, $[\mathbf{M}] \in G^{2k \times k}$ and $[\mathbf{T}] = [\mathbf{t}_1 | \cdots | \mathbf{t}_Q] \in G^{2k \times Q}$ where either $\mathbf{t}_i \leftarrow \mathsf{Span}(\mathbf{M})$ or $\mathbf{t}_i \leftarrow \mathbb{Z}_p^{2k}$, one can efficiently compute $[\mathbf{Z}]$, $[\mathbf{VZ}]$ and Q tuples $\big([\boldsymbol{\tau}_j], [\boldsymbol{\tau}'_j]\big)_{j \in [Q]}$ where $\mathbf{Z} \in \mathbb{Z}_p^{k \times k}$ is full-rank, $\mathbf{V} \in \mathbb{Z}_p^{k \times k}$ is a secret matrix, $\boldsymbol{\tau}_j \leftarrow \mathbb{Z}_p^k$, either $\boldsymbol{\tau}'_j = \mathbf{V}\boldsymbol{\tau}_j$ (when $\mathbf{t}_j \leftarrow \mathsf{Span}(\mathbf{M})$) or $\boldsymbol{\tau}'_j \leftarrow \mathbb{Z}_p^k$ (when $\mathbf{t}_j \leftarrow \mathbb{Z}_p^{2k}$).*

We are ready to prove Lemma 10.

Proof. Given $[\mathbf{M}]_1 \in G_1^{2k \times k}$ and $[\mathbf{T}]_1 = [\mathbf{t}_1 | \cdots | \mathbf{t}_q]_1 \in G_1^{3k \times q}$ where either $\mathbf{t}_j \leftarrow \mathsf{Span}(\mathbf{M})$ or $\mathbf{t}_j \leftarrow \mathbb{Z}_p^{2k}$, $\mathcal{B}$ proceeds as follows:

Generating q tuples. We invoke the algorithm described in Lemma 11 on input $(q, G_1, [\mathbf{M}]_1, [\mathbf{T}]_1)$ and obtain $\big([\mathbf{Z}]_1,\ [\mathbf{VZ}]_1,\ \big\{[\boldsymbol{\tau}_j]_1,\ [\boldsymbol{\tau}'_j]_1\big\}_{j \in [q]}\big)$.

Simulating pp. Sample $\mathbf{A}, \widehat{\mathbf{A}}, \widetilde{\mathbf{A}} \leftarrow \mathcal{U}_{3k,k}$ and randomly pick $\widehat{\mathbf{A}}^*$ and $\widetilde{\mathbf{A}}^*$, the respective bases of $\mathsf{Ker}\big((\mathbf{A}|\widetilde{\mathbf{A}})^\top\big)$ and $\mathsf{Ker}\big((\mathbf{A}|\widehat{\mathbf{A}})^\top\big)$. For all $i \in [n]$, pick $\bar{\mathbf{W}}_i \leftarrow \mathbb{Z}_p^{k \times 3k}$ and implicitly define

$$\mathbf{W}_i = \bar{\mathbf{W}}_i + \bar{\mathbf{V}} \cdot (\widehat{\mathbf{A}}^*)^\top$$

where $\bar{\mathbf{V}} = \mathbf{V}((\widehat{\mathbf{A}}^*)^\top \widehat{\mathbf{A}})^{-1} \in \mathbb{Z}_p^{k \times k}$. We can simulate PP from the observation

$$\mathbf{W}_i\mathbf{A} = \big(\bar{\mathbf{W}}_i + \bar{\mathbf{V}} \cdot (\widehat{\mathbf{A}}^*)^\top\big)\mathbf{A} = \bar{\mathbf{W}}_i\mathbf{A}.$$

Simulating $\widehat{h}_j^*$ and $\widetilde{h}_j^*$. It is direct to simulate all $\widehat{h}_j^*$ and $\widetilde{h}_j^*$ using $\widehat{\mathbf{A}}^*$ and $\widetilde{\mathbf{A}}^*$.

Simulating $\mathbf{h}_j \cdot (1_{\mathbb{H}_0};\ \widehat{h}_{1,j}^*, \ldots, \widehat{h}_{n,j}^*)$. Observe that

$$\mathbf{W}_i^\top \mathbf{r}_j + \widehat{\mathbf{A}}^* \widehat{\mathbf{r}}_{i,j} = \bar{\mathbf{W}}_i^\top \mathbf{r}_j + \widehat{\mathbf{A}}^*(\bar{\mathbf{V}}^\top \mathbf{r}_j + \widehat{\mathbf{r}}_{i,j}) \;\text{ for all } i \in [n], j \in [q'].$$

We can alternatively simulate $\mathbf{h}_j \cdot (1_{\mathbb{H}_0};\ \widehat{h}_{1,j}^*, \ldots, \widehat{h}_{n,j}^*)$ as $\bar{\mathbf{W}}_i^\top \mathbf{r}_j + \widehat{\mathbf{A}}^* \widehat{\mathbf{r}}_{i,j}$ for all $i \in [n], j \in [q']$ where $\mathbf{r}_j, \widehat{\mathbf{r}}_{i,j} \leftarrow \mathbb{Z}_p^k$ without secret matrix $\mathbf{V}$.

Simulating the challenge. Observe that

$$\mathbf{W}_i\widehat{\mathbf{A}} = \big(\bar{\mathbf{W}}_i + \bar{\mathbf{V}} \cdot (\widehat{\mathbf{A}}^*)^\top\big)\widehat{\mathbf{A}} = \bar{\mathbf{W}}_i\widehat{\mathbf{A}} + \mathbf{V}.$$

We can sample $\bar{\mathbf{s}}_j \leftarrow \mathbb{Z}_p^k$ and simulate the challenge as

$$\big(\big[\mathbf{A}\bar{\mathbf{s}}_j + \widehat{\mathbf{A}}\boldsymbol{\tau}_j\big]_1, \big[\bar{\mathbf{W}}_1\mathbf{A}\bar{\mathbf{s}}_j + \bar{\mathbf{W}}_1\widehat{\mathbf{A}}\boldsymbol{\tau}_j + \boldsymbol{\tau}'_j\big]_1, \ldots, \big[\bar{\mathbf{W}}_n\mathbf{A}\bar{\mathbf{s}}_j + \bar{\mathbf{W}}_n\widehat{\mathbf{A}}\boldsymbol{\tau}_j + \boldsymbol{\tau}'_j\big]_1\big).$$

Observe that, when $\mathbf{t}_j \leftarrow \mathsf{Span}(\mathbf{M})$, we have $\boldsymbol{\tau}'_j = \mathbf{V}\boldsymbol{\tau}_j$, the challenge is identical to $\{\mathbf{g}_j \cdot \widehat{\mathbf{g}}_j\}$; when $\mathbf{t}_j \leftarrow \mathbb{Z}_p^{2k}$, we have $\boldsymbol{\tau}'_j \leftarrow \mathbb{Z}_p^k$, the challenge is identical to $\{\mathbf{g}_j \cdot \widehat{\mathbf{g}}_j \cdot (1_{\mathbb{G}_0}; (g'_j)^{\mathbf{1}_n})\}$ where $\mathbf{s}'_j = \boldsymbol{\tau}'_j - \mathbf{V}\boldsymbol{\tau}_j$ is uniformly distributed over $\mathbb{Z}_p^k$. This proves the lemma. □

6 Concrete Constructions

We present our main result in Figure 1 whose adaptive security and anonymity in the MIMC setting is almost-tightly based on the k-Lin assumption.

```
$\mathsf{Param}(1^\lambda, n)$
$\mathbf{A} \leftarrow \mathcal{U}_{3k,k}$
for $(i,b) \in [n] \times \{0,1\}$ do
    $\mathbf{W}_{i,b} \leftarrow \mathbb{Z}_p^{k\times 3k}$, $\mathbf{Z}_{i,b} = \mathbf{W}_{i,b}\mathbf{A} \in \mathbb{Z}_p^{k\times k}$
$\textsc{gp} = \big([\mathbf{A}]_1, \{[\mathbf{Z}_{i,b}]_1, [\mathbf{W}_{i,b}]_2\}\big)$
return $\textsc{gp}$

$\mathsf{Setup}(\textsc{gp})$
$\boldsymbol{\alpha} \leftarrow \mathbb{Z}_p^{3k}$
$\textsc{mpk} = \big([\mathbf{A}]_1, \{[\mathbf{Z}_{i,b}]_1\}, [\mathbf{A}^\top\boldsymbol{\alpha}]_T\big)$
$\textsc{msk} = \big([\boldsymbol{\alpha}]_2, \{[\mathbf{W}_{i,b}]_2\}\big)$
return $\textsc{mpk}$, $\textsc{msk}$

$\mathsf{KeyGen}(\textsc{mpk}, \textsc{msk}, \textsc{id})$
$\mathbf{r} \leftarrow \mathbb{Z}_p^k$
$\textsc{sk} = \big([\mathbf{r}]_2, \big[\boldsymbol{\alpha} + \sum_{i=1}^n \mathbf{W}_{i,\textsc{id}[i]}^\top \mathbf{r}\big]_2\big) \in G_2^{4k}$
return $\textsc{sk}$

$\mathsf{Enc}(\textsc{mpk}, \textsc{id}, \textsc{m})$
$\mathbf{s} \leftarrow \mathbb{Z}_p^k$
$\textsc{ct}' = \big([\mathbf{As}]_1, \big[\sum_{i=1}^n \mathbf{Z}_{i,\textsc{id}[i]}\mathbf{s}\big]_1\big) \in G_1^{4k}$
$\textsc{key} = [\mathbf{s}^\top\mathbf{A}^\top\boldsymbol{\alpha}]_T \in G_T$
return $\textsc{ct} = (\textsc{ct}', \ \textsc{key} \cdot \textsc{m})$

$\mathsf{Dec}(\textsc{mpk}, \textsc{sk} = (\mathbf{k}_0, \mathbf{k}_1), \textsc{ct} = (\mathbf{c}_0, \mathbf{c}_1, c_2))$
return $\textsc{m} = c_2 \cdot e(\mathbf{c}_1, \mathbf{k}_0)/e(\mathbf{c}_0, \mathbf{k}_1)$
```

Fig. 1. Main result: A Concrete IBE Scheme Based on the k-Lin assumption.

Figure 2 presents a concrete instantiation of our main result based on SXDH (1-Lin) assumption by setting $k = 1$. Our description below only involves vectors and scalars.

```
$\mathsf{Param}(1^\lambda, n)$
$\mathbf{a} \leftarrow \mathbb{Z}_p^3$
for $(i,b) \in [n] \times \{0,1\}$ do
    $\mathbf{w}_{i,b} \leftarrow \mathbb{Z}_p^3$, $z_{i,b} = \langle \mathbf{w}_{i,b}, \mathbf{a}\rangle \in \mathbb{Z}_p$
$\textsc{gp} = \big([\mathbf{a}]_1, \big\{[z_{i,b}]_1, [\mathbf{w}_{i,b}]_2\big\}\big)$
return $\textsc{gp}$

$\mathsf{Setup}(\textsc{gp})$
$\boldsymbol{\alpha} \leftarrow \mathbb{Z}_p^3$
$\textsc{mpk} = \big([\mathbf{a}]_1, \big\{[z_{i,b}]_1\big\}, \big[\langle \mathbf{a}, \boldsymbol{\alpha}\rangle\big]_T\big)$
$\textsc{msk} = \big([\boldsymbol{\alpha}]_2, \big\{[\mathbf{w}_{i,b}]_2\big\}\big)$
return $\textsc{mpk}$, $\textsc{msk}$

$\mathsf{KeyGen}(\textsc{mpk}, \textsc{msk}, \textsc{id})$
$r \leftarrow \mathbb{Z}_p$
$\textsc{sk} = \big([r]_2, \big[\boldsymbol{\alpha} + r \cdot \sum_{i=1}^n \mathbf{w}_{i,\textsc{id}[i]}\big]_2\big) \in G_2^4$
return $\textsc{sk}$

$\mathsf{Enc}(\textsc{mpk}, \textsc{id}, \textsc{m})$
$s \leftarrow \mathbb{Z}_p$
$\textsc{ct}' = \big([s \cdot \mathbf{a}]_1, [s \cdot \sum_{i=1}^n z_{i,\textsc{id}[i]}]_1\big) \in G_1^4$
$\textsc{key} = [s \cdot \langle \mathbf{a}, \boldsymbol{\alpha}\rangle]_T$
return $\textsc{ct} = (\textsc{ct}', \textsc{key} \cdot \textsc{m})$

$\mathsf{Dec}(\textsc{mpk}, \textsc{sk} = (k_0, \mathbf{k}_1), \textsc{ct} = (\mathbf{c}_0, c_1, c_2))$
return $\textsc{m} = c_2 \cdot e(c_1, k_0)/e(\mathbf{c}_0, \mathbf{k}_1)$
```

Fig. 2. A Concrete IBE Scheme Based on SXDH ($k = 1$). Here we let $\langle \mathbf{x}, \mathbf{y}\rangle$ be the inner product of $\mathbf{x}$ and $\mathbf{y}$ of the same length and $e([\mathbf{x}]_1, [\mathbf{y}]_2) = [\langle \mathbf{x}, \mathbf{y}\rangle]_T$ in this case.

Acknowledgement. We want to thank Hoeteck Wee for his constructive suggestion and Kai Zhang for his useful advice. We also thank all anonymous reviewers of AsiaCrypt 2016 for their helpful comments. This work was supported by the National Natural Science Foundation of China (Grant No. 61373154, 61371083, 61472142, 61632012, 61672239, 61602180), the Prioritized Development Projects through the Specialized Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20130073130004), Shanghai High-tech field project (Grant No. 16511101400), Science and Technology Commission of Shanghai Municipality (Grant No. 14YF1404200), and the “Programme Avenir Lyon Saint-Etienne de l’Université de Lyon” in the framework of the programme “Investissements d’Avenir” (ANR-11-IDEX-0007).

References

1. Nuttapong Attrapadung. Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In *Advances in Cryptology–EUROCRYPT 2014*, pages 557–577. Springer, 2014.
2. Nuttapong Attrapadung. Dual system encryption framework in prime-order groups. *IACR Cryptology ePrint Archive*, 2015.
3. Nuttapong Attrapadung, Goichiro Hanaoka, and Shota Yamada. A framework for identity-based encryption with almost tight security. In *Advances in Cryptology–ASIACRYPT 2015*, pages 521–549. Springer, 2015.
4. Olivier Blazy, Eike Kiltz, and Jiaxin Pan. (hierarchical) identity-based encryption from affine message authentication. In *Advances in Cryptology–CRYPTO 2014*, pages 408–425. Springer, 2014.
5. Dan Boneh and Xavier Boyen. Efficient selective-id secure identity-based encryption without random oracles. In *Advances in Cryptology - EUROCRYPT 2004*, pages 223–238, 2004.
6. Dan Boneh and Xavier Boyen. Secure identity based encryption without random oracles. In *Advances in Cryptology - CRYPTO 2004*, pages 443–459, 2004.
7. Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In *Advances in CryptologyCRYPTO 2001*, pages 213–229. Springer, 2001.
8. Jie Chen, Romain Gay, and Hoeteck Wee. Improved dual system abe in prime-order groups via predicate encodings. In *Advances in Cryptology-EUROCRYPT 2015*, pages 595–624. Springer, 2015.
9. Jie Chen and Hoeteck Wee. Fully,(almost) tightly secure ibe and dual system groups. In *Advances in Cryptology–CRYPTO 2013*, pages 435–460. Springer, 2013.
10. Jie Chen and Hoeteck Wee. Dual system groups and its applications - compact HIBE and more. *IACR Cryptology ePrint Archive*, 2014:265, 2014.
11. Alex Escala, Gottfried Herold, Eike Kiltz, Carla Rafols, and Jorge Villar. An algebraic framework for diffie-hellman assumptions. In *Advances in Cryptology–CRYPTO 2013*, pages 129–147. Springer, 2013.
12. Romain Gay, Dennis Hofheinz, Eike Kiltz, and Hoeteck Wee. Tightly cca-secure encryption without pairings. In *Advances in Cryptology - EUROCRYPT 2016, Part I*, pages 1–27, 2016.
13. Craig Gentry. Practical identity-based encryption without random oracles. In *Advances in Cryptology - EUROCRYPT 2006*, pages 445–464, 2006.
14. Junqing Gong, Jie Chen, Xiaolei Dong, Zhenfu Cao, and Shaohua Tang. Extended nested dual system groups, revisited. In *Public-Key Cryptography–PKC 2016*, pages 133–163. Springer, 2016.
15. Jens Groth and Amit Sahai. Efficient noninteractive proof systems for bilinear groups. *SIAM Journal on Computing*, 41(5):1193–1232, 2012.
16. Dennis Hofheinz. Adaptive partitioning. *IACR Cryptology ePrint Archive*, 2016:373, 2016.

17. Dennis Hofheinz. Algebraic partitioning: Fully compact and (almost) tightly secure cryptography. In *Theory of Cryptography*, pages 251–281. Springer, 2016.
18. Dennis Hofheinz, Jessica Koch, and Christoph Striecks. Identity-based encryption with (almost) tight security in the multi-instance, multi-ciphertext setting. In *Public-Key Cryptography–PKC 2015*, pages 799–822. Springer, 2015.
19. Charanjit S Jutla and Arnab Roy. Shorter quasi-adaptive nizk proofs for linear subspaces. In *Advances in Cryptology-ASIACRYPT 2013*, pages 1–20. Springer, 2013.
20. Eike Kiltz and Hoeteck Wee. Quasi-adaptive nizk for linear subspaces revisited. In *Advances in Cryptology-EUROCRYPT 2015*, pages 101–128. Springer, 2015.
21. Allison Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In *Advances in Cryptology–EUROCRYPT 2010*, pages 62–91. Springer, 2010.
22. Allison Lewko and Brent Waters. New proof methods for attribute-based encryption: Achieving full security through selective techniques. In *Advances in Cryptology–CRYPTO 2012*, pages 180–198. Springer, 2012.
23. Benoit Libert, Marc Joye, Moti Yung, and Thomas Peters. Concise multi-challenge cca-secure encryption and signatures with almost tight security. In *Advances in Cryptology–ASIACRYPT 2014*, pages 1–21. Springer, 2014.
24. Benoît Libert, Thomas Peters, Marc Joye, and Moti Yung. Compactly hiding linear spans. In *Advances in Cryptology–ASIACRYPT 2015*, pages 681–707. Springer, 2015.
25. Moni Naor and Omer Reingold. Number-theoretic constructions of efficient pseudo-random functions. *J. ACM*, 51(2):231–262, 2004.
26. Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In *Advances in Cryptology–CRYPTO 2010*, pages 191–208. Springer, 2010.
27. Tatsuaki Okamoto and Katsuyuki Takashima. Adaptively attribute-hiding (hierarchical) inner product encryption. In *Advances in Cryptology–EUROCRYPT 2012*, pages 591–608. Springer, 2012.
28. Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure unbounded inner-product and attribute-based encryption. In *Advances in Cryptology–ASIACRYPT 2012*, pages 349–366. Springer, 2012.
29. Somindu C. Ramanna. More efficient constructions for inner-product encryption. In *ACNS 2016*, pages 231–248, 2016.
30. Somindu C. Ramanna and Palash Sarkar. Efficient adaptively secure IBBE from standard assumptions. *IACR Cryptology ePrint Archive*, 2014:380, 2014.
31. Somindu C. Ramanna and Palash Sarkar. Efficient (anonymous) compact HIBE from standard assumptions. In *Provable Security - 8th International Conference, ProvSec 2014, Hong Kong, China, October 9-10, 2014. Proceedings*, pages 243–258, 2014.
32. Adi Shamir. Identity-based cryptosystems and signature schemes. In *Advances in cryptology*, pages 47–53. Springer, 1985.
33. Brent Waters. Efficient identity-based encryption without random oracles. In *Advances in Cryptology - EUROCRYPT 2005*, pages 114–127, 2005.
34. Brent Waters. Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions. In *Advances in Cryptology-CRYPTO 2009*, pages 619–636. Springer, 2009.
35. Hoeteck Wee. Dual system encryption via predicate encodings. In *Theory of Cryptography*, pages 616–637. Springer, 2014.